United States
Environmental Protection
Agency

Office of Environmental Information
Office of Technology Operations & Planning
National Technology Services Division
Research Triangle Park, NC 27711

xxxx/xxx
December 17, 2004

SuSE Linux Enterprise Server 8 for IBM S/390 and IBM zSeries Standard Configuration Document

Draft

Draft

z/Linux for z/Series
Standard Configuration Document

December 17, 2004

The latest versions of the Security Checklist and the EPA Security Policy & Procedures supersede any conflicting security setting requirements or suggestions in this SCD. If there are questions on operating system security settings, call the Z/Linux System Support.

Draft

Prepared by
Z/Linux System Support

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
NATIONAL TECHNOLOGY SERVICES DIVISION
RESEARCH TRIANGLE PARK, NORTH CAROLINA

Warning

This Linux for zSeries Standard Configuration document covers only application servers including, but not limited to, servers running applications such as Oracle.

Draft

Table of Contents

REVISION HISTORY viii

1.0 INTRODUCTION 1

2.0 z/Linux System Support for z/Linux OS 3

3.0 VENDOR OVERVIEW 3
3.1 OPERATING SYSTEM REVISION HISTORY 4

4.0 VENDOR’S STANDARD SOFTWARE ENVIRONMENT 4
4.1 LINUX PATCHES 5
4.1.1 Patches Containing Security Fixes 5
4.2 SOFTWARE COMPONENTS 5
4.3 SUPPORTED HARDWARE 5

5.0 EPA STANDARD CONFIGURATION 6
5.1 SUPPORTED SYSTEMS 6
5.2 FILE SYSTEMS 7
5.3 KERNEL CONFIGURATION 7
5.4 COMMUNICATIONS SETUP 7
5.4.1 Linux for S/390 configuration files 8
5.4.2 Sendmail 8
5.4.3 Communications Services 8
5.4.3.1 xinetd 9
5.4.3.1.1 */etc/xinetd.conf* 9
5.4.3.2 inetd 9
5.4.3.3 TCP Wrappers and OpenSSH 9
5.4.3.3.1 */etc/hosts.allow* and */etc/hosts.deny* 10
5.4.3.3.2 */etc/syslog.conf* 11
5.4.3.4 Name Resolution 11
5.4.3.4.1 /etc/resolv.conf 11
5.4.3.4.2 /etc/hosts 11
5.5 SECURITY SETUP 11
5.5.1 File and Directory Permissions 12
5.5.1.1 System files 12
5.5.1.2 System configuration files 12
5.5.2 Console Security 12
5.5.3 EPA Warning Banner 13
5.5.4 Access Controls 13
5.5.4.1 Remote Access 13

5.5.4.1.1 */etc/hosts.equiv* 13
5.5.4.1.2 *.rhosts* or *.netrc* 14
5.5.4.2 Password Policy 14
5.5.4.3 Required Pluggable Authentication Module (PAM) configuration 16
5.5.4.3.1 */etc/pam.d/chage* 17
5.5.4.3.2 */etc/pam.d/chfn* 17
5.5.4.3.3 */etc/pam.d/chsh* 18
5.5.4.3.4 */etc/pam.d/login* 18
5.5.4.3.5 */etc/pam.d/other* 19
5.5.4.3.6 */etc/pam.d/passwd* 19
5.5.4.3.7 */etc/pam.d/sshd* 20
5.5.4.3.8 */etc/pam.d/su* 20
5.5.4.3.9 */etc/pam.d/useradd* 21
5.5.4.3.10 */etc/pam.d/vsftpd* 21
5.5.4.3.11 */etc/security/pam_pwcheck.conf* 22
5.5.4.3.12 */etc/security/pam_unix2.conf* 22
5.5.4.4 Setting up login controls 23
5.5.4.4.1 /etc/login.defs 23
5.5.4.4.2 Disable root login over the network 23
5.5.4.5 Update permissions for ’su’ 24
5.5.4.6 Sudo 24
5.5.4.7 SNMP 25
5.5.4.8 Automated Batch Processing (at, cron, batch, and anacron) 25
5.5.4.9 SSH secure shell 26
5.5.4.10 X 27
5.5.4.11 FTP 28
5.5.5 File Sharing and Central Authentication 29
5.5.5.1 NFS 30
5.5.5.2 NIS 31
5.5.5.3 Samba 31
5.5.5.4 LDAP 32
5.5.6 IP Configurations 32
5.5.7 Sendmail 32
5.5.8 SMTP 33
5.5.9 Auditing / System Logging (syslogd) 33
5.5.10 System Services 34
5.5.10.1 Allowed Open Ports 35
5.5.11 Configuration Tools 35
5.5.11.1 Tripwire 35
5.5.11.2 System Security Monitoring 35
5.5.11.3 linuxconf 36
5.5.11.4 Firewalls, ipchains and iptables 36
5.5.12 UNIX Security Checklist 36

5.6 STANDARD TOOLS 36
5.6.1 TOP System Usage Monitor 37
5.6.2 GCC "C" Compiler 37
5.6.3 PERL 37

Appendix A
EPA SOFTWARE INSTALLATION NOTES A-1
A.1 SOFTWARE UPGRADES A-1
A.2 NEW SOFTWARE INSTALLS A-3
A.3 LIST OF FILES TO MODIFY A-3

Appendix B
Secure Initial System Configuration B-1
B.1 Minimum packages to be installed B-1
B.2 Disable service B-2
B.3 Remove setuid/setgid root settings from binaries B-2

Appendix C
Monitoring, Logging & Audit B-4
C.1 Reviewing the system configuration B-4
C.2 System logging and accounting B-4
C.3 System configuration variables in /etc/sysconfig B-5

Appendix D
Pluggable Authentication Module (PAM) configuration B-9
D.1 Introduction to PAM configuration B-9

Appendix E
ONLINE FILES REFERENCE C-1

Appendix F
SYSTEM ADMINISTRATOR SKILLS REQUIREMENTS D-1

Appendix G
KEY CONTACTS AND UPDATES TO DOCUMENT E-1

Appendix H
ACRONYM LIST F-1

List of Tables

Table 1-2 EPA Support Status for z/Linux OS Revisions 2

Table 5-1 Sample */etc/hosts.allow* File 10

Table 5-2 Sample */etc/hosts.deny* File 10

Table 5-3 Sample */etc/resolv.conf* File 11

Table 5-4 Sample */etc/hosts* File 11

Table 5-5 Sample *chkconfig -l* Output 15

Table 5-6 Sample */etc/pam.d/chage* File 17

Table 5-7 Sample */etc/pam.d/chfn* File 18

Table 5-8 Sample */etc/pam.d/chsh* File 18

Table 5-9 Sample */etc/pam.d/login* File 19

Table 5-10 Sample */etc/pam.d/other* File 19

Table 5-11 Sample */etc/pam.d/passwd* File 20

Table 5-12 Sample */etc/pam.d/sshd* File 20

Table 5-13 Sample */etc/pam.d/su* File 21

Table 5-14 Sample */etc/pam.d/useradd* File 21

Table 5-15 Sample */etc/pam.d/vsftpd* File 22

Table 5-17 Sample */etc/security/pam_unix2.conf* File 22

Table 5-18 Sample */etc/login.defs* File 23

Table 5-19 Sample */var/spool/cron/allow* file 25

Table 5-20 Sample */etc/ssh/sshd_config* File 26

Table 5-21 Sample */etc/xinetd.conf* File 28

Table 5-22 Sample */etc/ftpusers* File 29

Table 5-23 Sample */etc/hosts.allow* Configuration File with Portmap 31

Table A-1 System Files Requiring Modification A-3

Table H-1 Key Contacts E-1

z/Linux Standard Configuration Document

REVISION HISTORY

No revisions at this time.

Draft

z/Linux
STANDARD CONFIGURATION DOCUMENT

1.0 INTRODUCTION

The purpose of a Standard Configuration Document (SCD) for any Operating System (OS) is to provide standards for protecting the EPA network and the systems attached to the network. The SCD's cover the minimum configuration and security requirements for connecting to EPA's network. All OS's connected to any part of the EPA network or any sub-net must comply with the appropriate SCD.

This SCD is written for trained, experienced system administrators (SA's). It is the responsibility of the IBM Systems Group to maintain trained, functional and informed SA's, not this SCD.

EPA security documents, vendor update/upgrade web sites, installation instructions, and security web sites are referenced in each SCD for the use of the SA's. The information in these documents and web sites is NOT duplicated in the SCD's because this would introduce update/version conflicts within the documentation and would increase the risks of security violations. Links to trusted sources are explicitly provided in the SCD's to ensure that patches come directly to the SA. The EPA OS security checklists take precedence over the SCD.

Information supplied in the appendix may not be current and is for reference only. This SCD covers only the EPA z/Linux Enterprise OS running many varied applications in only one location. Satisfying the varied operational needs, in conformity with EPA security policies and procedures, is the responsibility of Z/Linux System Support. Z/Linux System Support is responsible for SA support as well as the integrity and security of distributed systems. System users and administrators are responsible for their systems' effectiveness.

The SCD's do not:

- Duplicate the basic knowledge required of qualified system administrators.
- Cover mission application operating procedures.
- Recommend application software, the choice of GUI or shell, or other mission requirement software.
- Provide OS installation instructions.
- Cover administrative and management duties and procedures beyond the technical security and network attachment requirements.
- Provide a central EPA source for operating system or application software.
- Mitigate the duties and responsibilities of administrators', SIRMO's and ISO's.

The <u>z/Linux Standard Configuration Document</u> (SCD) is designed to minimize variances in

Environmental Protection Agency (EPA) equipment that can increase support time and cause unstable network connectivity. A Linux OS Standard Configuration document is required for every National Technology Services Division (NTSD)-supported version of an operating system. Standard configuration documents provide an EPA-defined baseline of vendor-provided products (e.g., OS, windowing subsystems, user desktop tools, and communications subsystems), and required vendor patches to these products, which are used to meet EPA standards for system configurations. Compliance with these standards is mandatory for connection of any system to the EPA's Wide Area Network (WAN). This document also contains recommendations for optional patches, system configurations, and EPA-specific OS installation instructions.

This SCD is targeted for readers experienced in the configuration, management, and administration of z/Linux systems. The EPA trained z/Linux system administrators, the intended audience for Linux OS Standard Configuration documents, will use these documents to ensure that their equipment is in compliance with EPA OS standard configurations. Secondary audiences, NTSD's Security and Telecommunications support personnel, are responsible for reviewing these standard configurations to ensure compliance with EPA policies and procedures.

The process of generating a standard configuration document involves a number of steps. These include, but are not limited to, the following:

1 Install target OS and configure to meet EPA security and communications standards.
2 Perform standard software regression testing of target OS. Not done initially.
3 Pilot use of target OS as required.
4 Identify and resolve critical problems with target OS.
5 Generate a standard configuration document.
6 Review a standard configuration document within NTSD.
7 Forward the final standard configuration document to the Deputy Chief Information Officer for Technology (DCIOT) for approval.
8 Release a standard configuration document upon approval from the DCIOT.

The support life-cycle for an OS version includes pilot testing, general support, senescent or minimal support, and termination of support. The pilot testing began in October 2001 and currently at the Generate a standard configuration document stage. Because there will be a standard configuration document for each supported version of an OS, each of these documents will also have a life-cycle. Table 1-2, EPA Support Status for z/Linux OS Revisions, provides a summary of the status of operating systems for S/390 and zSeries based z/Linux Enterprise servers within the EPA.

Table 1-2 EPA Support Status for z/Linux OS Revisions

Operating System Revision	Begin General Support	Begin Senescent Support	Support Ends
z/Linux for zSeries	10/2004	TBD	TBD
*Estimated dates (Dates for unsupported may be delayed but not advanced)			

2.0 z/Linux System Support for z/Linux OS

The Z/Linux System Support group provides the EPA with services centering around the use of the SuSE Linux Enterprise servers. The primary mission of Z/Linux System Support is to facilitate the accomplishment of z/Linux customers' mission by providing proactive leadership, management, and technical support through the incorporation of Open Systems within the EPA computing environment. Z/Linux System Support is responsible for SA support as well as the integrity and security of distributed systems.

Components of the Z/Linux System Support service include:

- Provide SA services to assist z/Linux application administrators in system configuration and optimization.
- Provide SA services to support Linux and TCP/IP network management.
- Propagation of new z/Linux OS releases, including the preparation of the z/Linux Standard Configuration Document.
- Maintenance of EPA online library for Linux software and documents.
- Linux technology assessment.
- EPA z/Linux implementation.

Appendix G, Administrator Skills Requirements for minimum requirements.

Appendix H, Key Contacts and Updates to Document, provides a summary of key Z/Linux System Support contacts.

3.0 VENDOR OVERVIEW

z/Linux for zSeries is a port of Linux to the zSeries architecture. Z/Linux for zSeries is a "pure" Linux from a user point of view. It supports the zSeries processor architecture and some devices that are specific to zSeries environments. Therefore, z/Linux for zSeries automatically inherits important strengths and reliability features of the zSeries hardware.

There are a number of venders providing z/Linux operating systems. SuSE Linux System Enterprise Server 8 (SLES 8) has been chosen for this z/Linux Standard Configuration Document.

This section provides an overview of SuSE, Inc., the premiere company that is marketing and supporting the 'Open Source' Linux operating system and related products. The company can be contacted at:

SuSE, Inc.
1100 Sansome Street

San Francisco, CA 94111
USA
Phone: (888) 875-4689
FAX: (415) 591-6619
SuSE website: http://www.suse.com/us/index.html

3.1 OPERATING SYSTEM REVISION HISTORY

This is initial implementation of SuSE Linux System Enterprise Server. Revision History will be available for subsequent versions of this Standard Configuration Document. SuSE Linux System Enterprise Server 8 is not an operating system per se, but rather a complete user environment. It consists of the following components:

- Linux kernel and related utilities
- XFree86 4.2.0
- a wide selection of desktop (graphical) environments and window managers, including the popular KDE 3.0 and Gnome 1.4 desktop environments
- a wide variety of tools and applications to manage the following items:
  - networking
  - security
  - printing
  - file management and sharing
  - local and centralized authentication and password control
  - DNS and DHCP client and server functionality
  - interoperability with UNIX, Microsoft Windows, and Novell NetWare operating systems
  - all of the other functions normally associated with an operating system
- a variety of database and office applications
- multimedia applications
- Apache web server

4.0 VENDOR’S STANDARD SOFTWARE ENVIRONMENT

This section describes the SuSE Linux System Enterprise Server 8 (SLES 8) version of the operating environment supported by Z/Linux System Support. This includes the OS revision level and various patches that are required and recommended. The EPA standard configuration, as discussed in Section 5.0 of this document, is predicated upon the z/Linux software environment.

4.1 LINUX PATCHES

This subsection describes the patches that Z/Linux System Support recommends installing as part of a baseline configuration.

4.1.1 Patches Containing Security Fixes

The current version of the kernel, 2.4.21-83, released by SuSE for SuSE Linux System Enterprise Server 8 of the operating system—or any subsequently released version—be installed on all EPA systems immediately after installation of the base operating system and the required upgrade to RPM. To determine the version of the kernel currently running on a system, the following command can be used:

```
uname -r
```

To determine the version installed per the RPM database, the following command can be used:

```
rpm -qa | grep kernel
```

If the version shown by the **rpm** command differs from the kernel currently running, it will be necessary to reboot the system to activate the newer kernel.

4.2 SOFTWARE COMPONENTS

The standard components of SuSE Linux System Enterprise Server 8 include the Linux kernel version 2.4.21-83 or higher, XFree86 4.0.3, RPM 4.04, Gnome 1.4, KDE 3.0 with kdelibs, and various other modules and tools included in the "official" release. Any Linux distribution other than SuSE is not supported. Should a computer with an unsupported version of the OS be suspected of causing a network problem, it may be disconnected from the EPA network.

Please note that while the 2.4.21-83 kernel ships with SuSE Linux System Enterprise Server 8, this document requires the installation of all security-related kernel upgrades or patches, as discussed in Section 4.3.1. The minimum acceptable version of the kernel is the latest version recommended by SuSE, Inc., currently 2.4.21-83, which is subject to change should any security vulnerability come to light.

4.3 SUPPORTED HARDWARE

SuSE Linux Enterprise Server 8 for S/390 and zSeries supports IBM's zSeries, G5 and G6 servers in 31-bit mode, and zSeries in 64-bit mode

CPU types

- eServer zSeries 800, 900 and 990
- S/390 Parallel Enterprise Servers Generation 6
- Processors can be CP (central processor) or IFL (integrated facility for Linux) engines

Network interfaces

- HiperSockets (iQDIO)
- OSA-Express Fast Ethernet and Gigabit Ethernet (QDIO)
- IUCV (VM DIAG)

I/O support

- ECKD DASD: 3390, and VM minidisk

IPL methods

- Post-installation: IPL from installed DASD

5.0 EPA STANDARD CONFIGURATION

The purpose of an EPA standard configuration is to minimize variances in the EPA z/Linux server systems that can increase the time needed for problem resolution and can produce unstable network connectivity. Systems that are attached to EPA's computer networks must be configured as defined in this document. Failure to follow the configuration guidelines may result in non-compliant systems being removed from the network.

5.1 SUPPORTED SYSTEMS

Z/Linux System Support will test the z/Linux servers running SuSE Linux Enterprise Server 8 (SLES 8). This standard operating system document was developed based on testing conducted on a z/VM virtual machines. The SuSE Linux Enterprise Server 8 platform is supported by Z/Linux System Support, provided that all hardware configurations in the system in question are both compatible and supports z/Linux. Table 5-1, below, lists EPA's minimum requirements for systems running z/Linux.

Z/Linux System Support will:

- provide System Administration (SA) support,

- install all of the security related kernel upgrades and patches,
- evaluate and install all appropriate installed system component upgrades and patches.

5.2 FILE SYSTEMS

This section provides recommendations for the placement of third-party, public domain, and nonstandard Linux software within the Linux file system structure. It is important to place software in standard locations to allow standardization of software installation instructions provided by Z/Linux System Support and to improve the ability of Z/Linux System Support to assist the z/Linux system administrator in solving problems.

If no location is defined in the installation notes for the software to be installed, it is recommended that the software be placed in ***/usr/local***. Executables should be placed in ***/usr/local/bin***. Libraries should be placed in ***/usr/local/lib***.

Most software will include installation instructions defining the installation location. The instructions should be followed. If space does not allow the software to be installed as instructed, the software should be installed in another file system and a link created to the directory specified in the installation documentation.

5.3 KERNEL CONFIGURATION

z/Linux is shipped with a modular kernel by default. Most hardware is handled by loadable modules called by initialization scripts at boot up. SuSE Linux Enterprise Server 8 does not require a kernel configuration. Upgrading the kernel is required when a security-related kernel upgrade is issued specifically for SuSE Linux Enterprise Server 8 by SuSE, Inc. The most recent supported kernel provided by SuSE, Inc. for SuSE Linux Enterprise Server 8 should be used unless a specific change is required.

Z/Linux System Support as the SA will be responsible for a kernel configuration and upgrading.

5.4 COMMUNICATIONS SETUP

The communications setup is defined by the communications architecture in the network within which the system operates. If the communications setup is incorrect, interoperability will suffer, interfaces to external resources will be inconsistent, support for the device will be difficult, and, in the worst case, the system may be disconnected from the EPA Wide Area Network. Consequently, known and tested communications configurations are essential. The communication hardware used to connect to the network will be an OSA Express ethernet card.

Note: IPv6 is not yet supported by the EPA and should not be installed at this time.

There are several ways to connect a z/Linux virtual machine to a physical network or to other Linux for z/Linux virtual machines. Three network drivers are provided with z/Linux:

- LAN Channel Station (LCS)
- Channel-to-channel (CTC)
- Inter-User Communications Vehicle (IUCV)

LCS will be provided to connect the z/Linux running in a z/VM virtual machine to the network directly through to the Open System Adapter (OSA). A virtual network using z/VM VLAN support will be provided to allow a group of z/Linux image’s network together.

5.4.1 Linux for S/390 configuration files

The following two files are used by the script ***/etc/init.d/network*** to initialize networking with the proper settings for the SuSE Linux Enterprise Server 8.

- The file ***/etc/HOSTNAME*** contains the primary name (i.e., hostname) of the Linux server.
- The file ***/etc/sysconfig/network/ifcfg-eth0*** contains basic network parameters for the ethernet card.
- The file ***/etc/hosts*** contains information regarding the known hosts on the Internet. Domain Name Services (DNS) has been used to get a more global perspective of the IP network. If DNS is not utilized, all known hosts must be defined in this file.

5.4.2 Sendmail

Sendmail, as provided in SuSE Linux Enterprise Server 8, can be utilized in the EPA environment. Within the EPA, Sendmail is used by the system administrators to process scheduled system reports and to export log files. This does not require running Sendmail as a daemon. Z/Linux System Support will disable Sendmail unless explicitly required for normal operations. See Section 5.5.7 Sendmail.

Note: Lotus Notes is the primary and preferred method for sending email within the EPA. Most EPA employees and contractors are provided a desktop workstation for email and administrative use. However, for those administrators who do not have a desktop, Sendmail may be used for official correspondence if Lotus Notes is not available.

5.4.3 Communications Services

The standard configuration uses either ***xinetd*** or ***inetd*** and the **tcpd** (tcp wrappers program) to limit access by remote machines and to record remote access attempts. ***Xinetd*** is a secure, powerful and efficient replacement for ***inetd*** and **tcpd**. This security tool can control denial-of-access attacks by providing access control mechanisms for all services based on the address of the remote client that want to connect to the server as well as the ability to make services available based on time of access, extensive logging, and the ability to bind services to specific interfaces. Z/Linux System Support recommends using ***xinetd***.

5.4.3.1 xinetd

Xinetd is the super-server that starts other servers that provide network services, such as file transfer, between systems. The file ***/etc/xinetd.conf*** contains only global default settings for all services. Each service formerly configured in the ***/etc/inetd.conf*** file now has a separate configuration file. While it remains possible to configure **xinetd** services directly in the ***/etc/xinetd.conf*** file, this is no longer the preferred method. Instead, Z/Linux System Support recommends using individual configuration files. The location of these files is determined by the include dir attribute on the last line of ***/etc/xinetd.conf***. Z/Linux System Support will not enable **xinetd**.

5.4.3.1.1 */etc/xinetd.conf*

The standard configuration will be configured with ***/etc/xinetd.conf*** for an ftp and telnet daemon. ***/etc/xinetd.conf*** will be only readable and writeable by root (Chmod 400 ***/etc/xinetd.conf***).

Checklist Item: ***/etc/xinetd.conf*** will be only readable and writeable by root.

5.4.3.2 inetd

inetd is a TCP/IP daemon that starts at system initialization and listens on all service ports for the services listed in its configuration file ***/etc/inetd.conf***. Z/Linux System Support will not enable **inetd**.

5.4.3.3 TCP Wrappers and OpenSSH

The **tcpd 7.6** (tcp wrappers package) can monitor and filter incoming requests for the SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, TALK, and other network services.

The package provides tiny daemon wrapper programs that can be installed without any changes to existing software or to existing configuration files. The wrappers report the name of the client host and of the requested service; the wrappers do not exchange information with the client or server applications, and impose no overhead on the actual conversation between the client and server applications.

Checklist Item: TCP wrappers are installed and in compliance with SCD.

5.4.3.3.1 */etc/hosts.allow* and */etc/hosts.deny*

The ***hosts.allow*** and ***hosts.deny*** files are configuration files for the tcp wrappers and OpenSSH access control software. These files control access to network daemons by remote clients. Although these files can be configured to trap remote access attempts, the standard configuration simply allows access to the network daemons only by EPA computers. If a greater level of security is desired, access controls can be further limited to specific system IP addresses within EPA. Table 5-1 contains the standard configuration of the ***/etc/hosts.allow*** file with SSH access permitted from all EPA systems.

Table 5-1 Sample */etc/hosts.allow* File

File: */etc/hosts.allow*

```
# /etc/hosts.allow
# See `man tcpd´ and `man 5 hosts_access´ ...
:
#telnetd : 134.67.128.177, 161.80.125.124.
#ftpd :134.67.128.177 , 161.80.125.123.
sshd: 134.67. , 161.80. , 204.46. , 204.47.:
#rlogind : 127.0.0.1
#
# If this machine is a server, uncomment one line below and change the
# name to match the X-terminal (or any X terminal that boots
# using tftp) DO NOT GENERALIZE THIS CONDITION!!!!! Add as many
# specific hosts as are required to boot the X terminals/diskless
# workstations.
#
# tftpd : diskless.workstation.region.epa.gov
```

Table 5-2 Sample */etc/hosts.deny* File

File: */etc/hosts.deny*

```
# /etc/hosts.deny
# See `man tcpd´ and `man 5 hosts_access´ ...
# for a detailed description.
:
http-rman : ALL EXCEPT LOCAL
```

All connections and connection failures are logged in ***/var/log/secure***.

5.4.3.3.2 */etc/syslog.conf*

The file ***/etc/syslog.conf*** contains information used by the system log daemon, **syslogd**, to forward a system message to appropriate log files and/or users.

5.4.3.4 Name Resolution

5.4.3.4.1 /etc/resolv.conf

Name resolution is the act of resolving internet host names (fully qualified or otherwise) into IP addresses. The ***/etc/resolv.conf*** file is used by the resolver to determine the IP address for a host name.

Table 5-3 Sample */etc/resolv.conf* File

File: */etc/resolv.conf*

```
domain rtpnc.epa.gov
nameserver 134.67.208.10
```

5.4.3.4.2 /etc/hosts

As the z/Linux gets started, it will need to know the mapping of some hostnames to IP addresses before DNS can be referenced. This mapping is kept in the ***/etc/hosts*** file. In the absence of a name server, any network program on your system consults this file to determine the IP address that corresponds to a host name.

Table 5-4 Sample */etc/hosts* File

File: */etc/hosts*

```
#
# hosts         This file describes a number of hostname-to-address
:
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#
127.0.0.1       localhost
134.67.180.138    linux04.rtpnc.epa.gov linux04
```

5.5 SECURITY SETUP

All z/Linux servers within EPA must conform to Policy 200.03, NCC NT and UNIX Security, and the U.S. EPA NTSD UNIX Server Security Checklist. The guidelines outlined in this section conform to established security policies and documents.

The initial LINUX configurations will be configured for:

- A single application
- No end users will be allowed to logon to the LINUX system.
- Logon IDs will be limited to system administrators and application administrators.
- Only system administrators will be allowed to used root.

Note - Because of the limited access to the LINUX system, the security will rely on root authority to provide security.

5.5.1 File and Directory Permissions

Files and directories that comprise the operating system must have ownership and permission settings that prevent easy tampering. In general, write-access to these files must be reserved for the operating system equivalent of the system administrator or root.

5.5.1.1 System files

System files include, but are not limited to, those in directories ***/, /bin, /boot, /etc, /sbin, /usr/bin, /usr/etc, /usr/lib, /usr/share,*** and ***/usr/sbin***. Log files located in ***/var/log*** should have both read and write access restricted to root. Use the **chmod** command to change permissions as required. For example, to change the system security log to root-only read/write access, the command would be:

```
sudo chmod 600 /var/log/secure
```

5.5.1.2 System configuration files

System configuration files will be set so that write-access is restricted to root. System administrators should review all file systems that contain sensitive or system files to ensure that they are not world-readable (**chmod** to *640*).

All system device files must be located in the /dev directory and must be protected from unauthorized access. Disk devices such as ***/dev/mem*** and ***/dev/kmem*** must never be world-readable. Terminal devices must be owned by root with read and write access permissions for owner, group, and world when devices are not allocated.

5.5.2 Console Security

No configuration changes are required to secure the console in z/Linux. The system administrator should ensure that no entries have been made to the directory ***/etc/security***.

5.5.3 EPA Warning Banner

The following message must be displayed after the operating system level message:

> **WARNING NOTICE**
>
> **This is a United States Environmental Protection Agency (EPA) computer system, which may be accessed and used only for official Government business. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. All information on this computer system may be monitored, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including law enforcement. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms.**

The warning banner must be placed in the following files:

- ***/etc/motd*** the "the message of the day" banner,
- ***/etc/issue*** the login banner that gets displayed to local users,
- ***/etc/issue.net*** the login banner that users will see when they make a networked (i.e. telnet, SSH) connection to your machine.
- ***/etc/vsftp.conf*** the FTP login banner string.

Note: The ***/etc/ssh/sshd_config*** file has an entry Banner ***/etc/issue***.

5.5.4 Access Controls

Remote access to EPA servers should be restricted to systems that need access. The more tightly access is limited, the more secure a server becomes. The following sections are designed to make unauthorized access to EPA z/Linux servers as difficult as possible.

5.5.4.1 Remote Access

5.5.4.1.1 */etc/hosts.equiv*

No wild-cards may be permitted in the ***/etc/hosts.equiv*** file. Hosts in public access areas will not be included in ***/etc/hosts.equiv*** as trusted. ***/etc/hosts.equiv*** will be only readable and writeable by root (Chmod 600 ***/etc/hosts.equiv***).

Checklist Item: ***/etc/hosts.equiv*** will be only readable and writeable by root.
Checklist Item: No wild-carding is used in the "/etc/hosts.equiv" file.
Checklist Item: No local hosts that are located in public areas configured in the "/etc/hosts.equiv" file as "trusted.

5.5.4.1.2 *.rhosts* or *.netrc*

.***rhosts*** and .***netrc*** files must be placed on the system in the ***/root*** directory. Both files should have blank content, ownership set to root:root, and access completely restricted with the following command:

```
sudo chmod 0 /root/.rhosts  /root/.netrc
```

In addition, the system administrator should find all additional .***netrc*** and .***rhosts* files** on the system, remove their content, and revise the permissions as above. Due to the relatively serious security vulnerabilities related to ***.rhosts*** files, the system administrator should audit and monitor the status of these files in users' home directories on a regular basis.

Checklist Item: Files .rhosts and .netrc will exist, have blank content, and have chmod = 0

5.5.4.2 Password Policy

All EPA z/Linux servers within EPA must conform to Policy 200.03, NCC NT and UNIX Security in the U.S. EPA NTSD Operational Policies Manual regarding password length and password expiration. IBM Linux Systems Support will use the UNIX Server and Workstation Security checklists while configuring user password and expiration dates.

Shadow (encrypted) passwords should be chosen at install time. In addition, IBM Linux Systems Support will use md5 passwords to provide additional security. Again, this option should be chosen at system installation.

The **chage** command should be used to modify the ***/etc/shadow*** file to cause passwords to expire every 90 days and to issue a notice 10 days prior to expiration. The command format is:

```
sudo chage -M 90 -W 10 <username>
```

The file ***/etc/pam.d/login*** should be edited to force compliance with password requirements in the UNIX Standard Configuration Security Checklist, Section 2.0, (located at URL http://intranet.epa.gov/dss/DSS_Customer/SCD/unix-checklist.pdf) as shown in the following example, Table 5-5.

Table 5-5 Sample *chkconfig -l* Output

```
SuSEfirewall2_final      0:off   1:off   2:off   3:off   4:off   5:off   6:off
SuSEfirewall2_init       0:off   1:off   2:off   3:off   4:off   5:off   6:off
SuSEfirewall2_setup      0:off   1:off   2:off   3:off   4:off   5:off   6:off
apache                   0:off   1:off   2:off   3:off   4:off   5:off   6:off
argus                    0:off   1:off   2:off   3:off   4:off   5:off   6:off
atd                      0:off   1:off   2:on    3:on    4:off   5:on    6:off
audit                    0:off   1:off   2:on    3:on    4:off   5:on    6:off
boot.clock               0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.crypto              0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.idedma              0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.ipconfig            0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.klog                0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.ldconfig            0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.localfs             0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.localnet            0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.lvm                 0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.md                  0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.proc                0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.proc.orig           0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.restore_permissions 0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.scpm                0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.scsidev             0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.swap                0:off   1:off   2:off   3:off   4:off   5:off   6:off
boot.sysctl              0:off   1:off   2:off   3:off   4:off   5:off   6:off
chandev                  0:off   1:off   2:off   3:off   4:off   5:off   6:off
cron                     0:off   1:off   2:on    3:on    4:off   5:on    6:off
cups                     0:off   1:off   2:off   3:off   4:off   5:off   6:off
evlog                    0:off   1:off   2:off   3:off   4:off   5:off   6:off
fbset                    0:off   1:on    2:on    3:on    4:off   5:on    6:off
fdrupstream              0:off   1:off   2:on    3:on    4:on    5:on    6:off
gpm                      0:off   1:off   2:off   3:off   4:off   5:off   6:off
hotplug                  0:off   1:on    2:on    3:on    4:off   5:on    6:off
hsnc                     0:off   1:off   2:off   3:off   4:off   5:off   6:off
hwscan                   0:off   1:off   2:on    3:on    4:off   5:on    6:off
ippl                     0:off   1:off   2:off   3:off   4:off   5:off   6:off
mon                      0:off   1:off   2:off   3:off   4:off   5:off   6:off
nagios                   0:off   1:off   2:off   3:off   4:off   5:off   6:off
network                  0:off   1:off   2:on    3:on    4:off   5:on    6:off
nfs                      0:off   1:off   2:off   3:off   4:off   5:off   6:off
nscd                     0:off   1:off   2:off   3:on    4:off   5:on    6:off
portmap                  0:off   1:off   2:off   3:off   4:off   5:off   6:off
postfix                  0:off   1:off   2:off   3:on    4:off   5:on    6:off
powertweakd              0:off   1:off   2:off   3:off   4:off   5:off   6:off
random                   0:off   1:off   2:on    3:on    4:off   5:on    6:off
raw                      0:off   1:off   2:off   3:off   4:off   5:off   6:off
rpasswdd                 0:off   1:off   2:off   3:off   4:off   5:off   6:off
rpmconfigcheck           0:off   1:on    2:on    3:on    4:off   5:on    6:off
scanlogd                 0:off   1:off   2:off   3:off   4:off   5:off   6:off
snmpd                    0:off   1:off   2:off   3:off   4:off   5:off   6:off
sshd                     0:off   1:off   2:off   3:on    4:off   5:on    6:off
syslog                   0:off   1:off   2:on    3:on    4:off   5:on    6:off
xdm                      0:off   1:off   2:off   3:off   4:off   5:on    6:off
xfs                      0:off   1:off   2:off   3:off   4:off   5:off   6:off
xinetd                   0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

Information on the ***pam_cracklib*** module (referenced in the first password entry in ***/etc/pam.d/login***), which is used to enforce the requirements, can be found at: http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam-6.html#ss6.3.

Password checking against dictionary words must be enabled to improve password security.

The system administrator should disable or remove any unneeded system accounts and groups. Accounts that can and, in most cases, should be removed include the following:

adm
news
uucp
gopher
lp (if no printing will take place)
operator
sync (if not using rsync)
games (if not using X server)

The command for removing an account is:

sudo userdel <username>

Groups which can and, in most cases, should be removed include:

adm
news
uucp
dip
lp (if no printing will take place)
pppusers
games (if not using X server)

The command for removing a group is:

sudo groupdel <group name>

5.5.4.3 Required Pluggable Authentication Module (PAM) configuration

You MUST restrict authentication to services that are explicitly specified. The ’other’ fallback MUST be disabled by specifying the *pam_deny.so* module for each *module-type* in the ’other’ configuration. This ensures that access decisions within the PAM system are handled only by the service specific PAM configuration.

You MUST add the *pam_wheel.so* module to the ’auth’ *module type* configuration for the ’su’ service and specify the ’trusted’ group.

You MUST add the *pam_tally.so* module to the 'auth' *module type* configuration to disable accounts after a certain number of failed login attempts. Be aware that this can be used in denial-of-service attacks to lock out legitimate users.

You MUST NOT modify other settings, specifically you MUST use the 'md5' and 'use cracklib' options for the *pam__pwcheck.so* module.

The 'remember=XX' option must be added to the ***/etc/security/pam_pwcheck.conf*** file to force users to create new passwords and not re-use ones that they had previously, i.e. to prevent users from simply alternating between two passwords when asked to change it due to expiration. XX is any number between 7 and 400.

The system supports many other PAM modules apart from the ones shown here. In general, PAM modules that restrict logins further MAY be used. You MUST NOT weaken the login restrictions through configuration changes of the modules shown here or via additional modules.

Here are the pam configuration files:

5.5.4.3.1 */etc/pam.d/chage*

This file configures the access control for the **chage** command. It allows the use of chage only after the user's password has been entered or the calling user is 'root'.

Table 5-6 Sample */etc/pam.d/chage* File

File: */etc/pam.d/chage*

```
#%PAM-1.0
# root is allowed to use chage without authentication
auth        sufficient      pam_rootok.so
auth        required pam_unix2.so
account         required pam_unix2.so
password        required pam_pwcheck.so
password        required pam_permit.so
session         required pam_deny.so
```

5.5.4.3.2 */etc/pam.d/chfn*

This file configures the access control for the **chfn** command. It allows the use of **chfn** only after the user's password has been entered or the calling user is 'root'.

Table 5-7 Sample */etc/pam.d/chfn* File

File: */etc/pam.d/chfn*

```
#%PAM-1.0
auth        sufficient    pam_rootok.so
auth        required pam_unix2.so
Account     required pam_unix2.so
password    required pam_pwcheck.so
password    required pam_unix2.so use_first_pass use_authtok
session     required pam_deny.so
```

5.5.4.3.3 */etc/pam.d/chsh*

This file configures the access control for the **chsh** command. It allows the use of chsh only after the user’s password has been entered or the calling user is ’root’.

Table 5-8 Sample */etc/pam.d/chsh* File

File: */etc/pam.d/chsh*

```
#%PAM-1.0
auth        sufficient    pam_rootok.so
auth        required pam_unix2.so
account     required pam_unix2.so
password    required pam_pwcheck.so
password    required pam_unix2.so use_first_pass use_authtok
session     required pam_deny.so
```

5.5.4.3.4 */etc/pam.d/login*

This file configures the behavior of the *login* program. It allows root login only for terminals configured in ***/etc/securetty***. If the file ***/etc/nologin*** is present, then only root can log in. The optional *pam_env* module MAY be used to set environment variables from ***/etc/security/pam_env.conf***. The optional pam mail module MAY be used to notify the user that there is new mail. The *pam_tally* module MUST be used to block the user after 5 failed login attempts. The optional *pam_limits* module MAY be used to enforce resource limits via ***/etc/security/limits.conf***.

Table 5-9 Sample */etc/pam.d/login* File

File: */etc/pam.d/login*

```
#%PAM-1.0
auth        required pam_tally.so onerr=fail no_magic_root
auth        requisite     pam_unix2.so
auth        required pam_securetty.so
auth        required pam_nologin.so
auth        required pam_env.so # optional
auth        required pam_mail.so # optional
account     required pam_unix2.so
account     required pam_tally.so deny=6 reset no_magic_root
password    required pam_pwcheck.so
password    required pam_unix2.so use_first_pass use_authtok
session     required pam_unix2.so
session     required pam_limits.so # optional
```

5.5.4.3.5 */etc/pam.d/other*

This configuration applies for all PAM usage for which no explicit service is configured. It will block and log any attempts.

Table 5-10 Sample */etc/pam.d/other* File

File: */etc/pam.d/other*

```
#%PAM-1.0
auth        required pam_warn.so
auth        required pam_deny.so
account     required pam_warn.so
account     required pam_deny.so
password    required pam_warn.so
password    required pam_deny.so
session     required pam_warn.so
session     required pam_deny.so
```

5.5.4.3.6 */etc/pam.d/passwd*

This sevice configuration applies to password changes. Please see also ***/etc/security/pam_pwcheck.conf***.

Table 5-11 Sample */etc/pam.d/passwd* File

File: */etc/pam.d/passwd*

```
#%PAM-1.0
auth        required pam_unix2.so
account     required pam_unix2.so
password    required pam_pwcheck.so
password    required pam_unix2.so use_first_pass use_authtok
session     required pam_unix2.so
```

5.5.4.3.7 */etc/pam.d/sshd*

This file configures the PAM usage for SSH. This is identical to the *login* configuration except for the *securetty* entry which is not applicable to network logins.

Table 5-12 Sample */etc/pam.d/sshd* File

File: */etc/pam.d/sshd*

```
#%PAM-1.0
auth        required pam_tally.so onerr=fail no_magic_root
auth        required pam_unix2.so
auth        required pam_nologin.so
auth        required pam_env.so # optional
account     required pam_unix2.so
account     required pam_nologin.so
account     required pam_tally.so deny=6 reset no_magic_root
password    required pam_pwcheck.so
password    required pam_unix2.so use_first_pass use_authtok
session     required pam_unix2.so
session     required pam_limits.so # optional
```

5.5.4.3.8 */etc/pam.d/su*

This file configures the behavior of the **su** command. Only users in the trusted group can use it to become ’root’, as configured with the *pam_wheel* module.

Table 5-13 Sample */etc/pam.d/su* File

File: */etc/pam.d/su*

```
#%PAM-1.0
auth        sufficient   pam_rootok.so
auth        required pam_wheel.so use_uid group=trusted
auth        required pam_unix2.so
auth        required pam_tally.so onerr=fail no_magic_root
account     required pam_unix2.so
account     required pam_tally.so no_magic_root # deny=5 reset
password    required pam_unix2.so
session     required pam_unix2.so
```

Forcing the root user to change the root password is not desired here, therefore the *pam_pwcheck.so* module is absent.

5.5.4.3.9 */etc/pam.d/useradd*

This file allows the root user to add accounts without entering the root password.

Table 5-14 Sample */etc/pam.d/useradd* File

File: */etc/pam.d/useradd*

```
#%PAM-1.0
auth        sufficient   pam_rootok.so
auth        required pam_deny.so
account     required pam_permit.so
password    required pam_permit.so
session     required pam_deny.so
```

Forcing the root user to change the root password is not desired here, therefore the *pam_pwcheck.so* module is absent.

5.5.4.3.10 */etc/pam.d/vsftpd*

This file configures the authentication for the FTP daemon. With the listfile module, users listed in **/etc/ftpusers** are denied FTP access to the system.

Table 5-15 Sample */etc/pam.d/vsftpd* File

File: */etc/pam.d/vsftpd*

```
#%PAM-1.0
auth         required pam_tally.so onerr=fail no_magic_root
auth         required pam_listfile.so item=user sense=deny \file=/etc/ftpusers onerr=fail
auth         required pam_unix2.so
account      required pam_unix2.so
account      required pam_tally.so deny=6 reset no_magic_root
password     required pam_unix2.so
session      required pam_unix2.so
```

Note that the FTP protocol has no provisions for changing passwords, therefore the *pam_pwcheck.so* module is absent.

5.5.4.3.11 */etc/security/pam_pwcheck.conf*

This file contains the default option for the *pam_pwcheck* module. This makes it easier to set a global policy. The *md5* option enables long passwords (up to 127 characters, see also the limit in ***/etc/login.defs***, and the *use cracklib* option activates password quality checks against standard dictionary and permutation attacks. The *remember* option ensures that the user does not reuse passwords by keeping track of the specified number of previously used passwords in the file ***/etc/security/opasswd***.

Table 5-16 Sample */etc/security/pam_pwcheck.conf* File

File: */etc/security/pam_pwcheck.conf*

```
password:    md5 use_cracklib remember
```

5.5.4.3.12 */etc/security/pam_unix2.conf*

This file contains the default option for the *pam_unix2* module. This makes it easier to set a global policy. The *md5* option enables long passwords (up to 127 characters, see also the limit in ***/etc/login.defs***. The *trace* option activates session tracing (start/stop) via *syslog*.

Table 5-17 Sample */etc/security/pam_unix2.conf* File

File: */etc/security/pam_unix2.conf*

```
auth:
account:
password:    md5
session:  trace
```

5.5.4.4 Setting up login controls

5.5.4.4.1 /etc/login.defs

The system supports various options to control log ins in ***/etc/login.defs***. The UMASK entry sets the default umask to the most restrictive setting. Users and processes MAY override this setting as required, i.e. through a setting in their personal shell profile or a service-specific configuration file.

Table 5-18 Sample */etc/login.defs* File

File: */etc/login.defs*		
LASTLOG_ENAB	yes	Log last log in
OBSCURE_CHECKS_ENAB	yes	Enable more strict password checks
UMASK	077	Default File permission mask
PASS_MAX_DAYS	60	Maximum password life time (<= 60)
PASS_MIN_DAYS	1	Minimum password life time (0 < PASS_MIN_DAYS < PASS_MAX_DAYS)
PASS_MIN_LEN	8	Minimum password length (MUST be at least 8)
PASS_WARN_AGE	5	Warn days before expiry
CRACKLIB_DICTPATH	/usr/lib/cracklib_dict	Base name of the cracklib library
LOGIN_RETRIES	3	Retries before the login process is killed
LOGIN_TIMEOUT	60	Max time in seconds per login attempt
PASS_CHANGE_TRIES	3	Max attempts at changing passwords
PASS_ALWAYS_WARN	yes	Warn even root about weak passwords
PASS_MAX_LEN	127	Maximum usable length of password
CHFN_AUTH	yes	Require password for chfsn/chsh
CHFN_RESTRICT	rwh	Fields that chfn may change
DEFAULT_HOME	no	Disallow login without home directory

5.5.4.4.2 Disable root login over the network

Login from the network with user ID 0 ('root') MUST NOT be permitted over the network. Administrators MUST use an ordinary user ID to log in, and then use the ***/bin/su*** - command to switch identities. For more information, refer to the section "Gaining superuser access" (§4.3) below.

It is recommended that administrators are reminded of this by adding the following alias to the bash configuration file ***/etc/bash.bashrc.local*** that disables the pathless '**su**' command:

```
alias su="echo \"Always use '/bin/su -' (see Security Guide)\""
```

This alias can be disabled for the root user in ***/root/.bashrc***:

```
unalias su
```

The restriction for direct root logins is enforced through two separate mechanisms. For network logins using ssh, the PermitRootLogin no entry in ***/etc/ssh/sshd_config*** MUST be set (see next section). Console and serial terminal logins use the pam securetty.so PAM module in the ***/etc/pam.d/login*** file, which verifies that the terminal character device used is listed in the file ***/etc/securetty***.

5.5.4.5 Update permissions for ’su’

The ’su’ binary MUST be restricted to members of the ’trusted’ group. This will be enforced both with PAM configuration (configured later) and the binary’s permissions.

```
chgrp trusted /bin/su
chmod 4710 /bin/su
```

When running the chkstat command as described above, this will be configured automatically.

5.5.4.6 Sudo

The “**sudo**” program must be implemented to limit root access by users and to record root access attempts and usage. **Sudo** allows a permitted user to execute a command as the superuser (real and effective uid and gid are set to 0 and root's group, as set in the passwd file respectively).

Sudo determines who is an authorized user by consulting the file ***/etc/sudoers*** or ***/usr/local/etc/sudoers***. By giving **sudo** the *-v* flag, a user can update the time stamp without running a command. The password prompt itself will also time out if the password is not entered within N minutes. (Again, this is defined at installation time and defaults to 5 minutes.)

If an unauthorized user executes **sudo**, mail will be sent from the user to the local authorities (defined at installation time). **sudo** was designed to log via the 4.3 BSD *syslog(3)* facility but can log to a file instead if so desired (or to both syslog and a file).

The current version of **sudo** can be found at http://www.courtesan.com/sudo. Z/Linux System Support will checking this site regularly for updates to ensure that the most recent and most secure version is being used.

When **sudo** is installed, the users that will be using root access for that machine will need to be added. The sudoers man page provides information on how to grant rights to each user. To use **sudo**, one types:

```
sudo <command>
```

The system will then ask for a password, which is the user's password for his/her account.

5.5.4.7 SNMP

Simple Network Management Protocol (SNMP) is used for monitoring events and detecting problems on a network. SuSE Linux Enterprise Server 8 ships with a large variety of SNMP utilities and protocol tools from the University of California-Davis (UCD) SNMP project, version 4.1.2.

Z/Linux System Support will disable SNMP (smpd daemon) unless it is required for system monitoring, or unless application software specifically requires SNMP.

If SNMP is used, the system administrator must edit the ***/etc/snmpd.conf*** file and change the community string from *community public 0.0.0.0 read* to *community <STRING> a.b.c.d read* where *STRING* is a nontrivial phrase and *a.b.c.d* is the IP address of the specific server allowed to perform SNMP queries on the system. In addition, the following command must be issued:

```
sudo chmod 640 /etc/snmpd.conf
```

to ensure that the configuration file is not world-readable and that only root may write to the file.

Checklist Item: If SNMP is enabled, the SNMP community name will be non-trivial .

5.5.4.8 Automated Batch Processing (at, cron, batch, and anacron)

Linux provides the system administrator with a large number of options for automating system tasks. These facilities run as root and must be restricted to root and, if required, to privileged users with a thorough understanding of UNIX batch processing. Table 5-12 shows sample ***/var/spool/cron/allow*** file. In this example, only root is allowed access. If **at** is used, an identical file named ***/etc/at.allow*** must be created to restrict access.

Table 5-19 Sample */var/spool/cron/allow* file

File: */var/spool/cron/allow*
root

at provides much of the same functionality as **cron**, but has much poorer security. Z/Linux System Support will not supporting **at** and will disable the **atd** daemon.

Checklist Item: Access to **cron** will be limited.
Checklist Item: Access to **at** will be limited.

5.5.4.9 SSH secure shell

SSH secure shell provide secure encrypted communications between two untrusted hosts over an insecure network. **PrintLastLog yes** will be set in ***/etc/ssh/sshd_config*** to display last logon. The SSH Server will be configured to reject attempts to log in as root. The authentication mechanisms other than User/Password MUST be disabled. The setting PAMAuthenticationViaKbdInt MUST be disabled, since this would otherwise circumvent the disabled root logins over the network. This results in the following option set for the SSH daemon that MUST be set in ***/etc/ssh/sshd_config***:

Checklist Item: Last login will be displayed.

Table 5-20 Sample */etc/ssh/sshd_config* File

File: */etc/ssh/sshd_config*

```
# This is the sshd server system-wide configuration file.  See sshd(8)
# for more information.

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
Protocol 2,1
:
# Authentication:

#LoginGraceTime 600
PermitRootLogin no
#StrictModes yes

RSAAuthentication no
PubkeyAuthentication no
:
# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
:
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
PermitEmptyPasswords no

# Change to no to disable s/key passwords
```

File: */etc/ssh/sshd_config*

```
ChallengeResponseAuthentication no

# Kerberos options
KerberosAuthentication no

# GSSAPI options
GSSAPIAuthentication no

# Warning: enabling this may bypass the setting of 'PasswordAuthentication'
PAMAuthenticationViaKbdInt no

X11Forwarding no
:
PrintLastLog yes
:
# no default banner path
Banner /etc/issue

# override default of no subsystems
Subsystem     sftp /usr/lib/ssh/sftp-server
```

5.5.4.10 X

SuSE Linux Enterprise Server 8 uses **xauth** by default to control access to the X Windows System. The **.Xauthority** file in each user's home directory contains the display names followed by a hexadecimal number (the "magic cookie"), which is read by the X server. If the cookie matches the one in memory, access to the display is granted. System administrators should not disable **xauth**, nor should they permit users to do so. Specifically, the **xhost +** command, for disabling access control, may not be used. Permissions on the **.Xauthority** files should be set to *600*.

XDCMP is used on systems that act as an X-server for remote X-terminals. It is also used to allow graphical access from Windows systems using remote X software such as Hummingbird Exceed, WRL Reflection X, or eXcursion. If remote X access is not required, it should be disabled. This can be accomplished by commenting out the *CHOOSER BROADCAST* line in ***/etc/X11/xdm/Xaccess.***

Remote X access is required for SA to use services like YaST. Remote X access will be limited to a small number of remote clients, the system administrator should limit it to specific hosts by uncommenting the *CHOOSER %hostlist* line and including a list of permitted hosts.

The system administrator will configures the server to boot to run level 5 (graphical login), the EPA Warning Banner shown in Section 5.5.3 must be displayed by either **gdm** (for systems using Gnome as the default desktop environment), **kdm** (if using KDE as the default desktop environment), or **xdm** (if neither Gnome nor KDE are installed).

Under GNOME the system administrator must modify the file ***/etc/opt/gnomes2/gdm.conf***. The string to change is *Welcome*, in the [greeter] section. The banner text should be typed in a single string and \n used to add line breaks.

Under KDE the system administrator will need to modify the file ***/etc/opt/kde3/share/config/kdm/kdmrc***. This file provides configuration information for **kdm**, the KDE Desktop Manager. The field that needs to be modified, the *GreetString*, is about halfway down the file. Because of the length of the EPA Warning Banner, the KDE Control Center should not be used to configure the greeting string. Line breaks can be inserted into the text output only if **kdmrc** is edited with vi. Line breaks may be added by simply inserting \n where the breaks need to occur.

Checklist Item: Magic Cookie host authentication will be in place.
Checklist Item: The **xhost +** command will be disabled.
Checklist Item: The EPA approved warning banner will be in place for an Telnet server .

5.5.4.11 FTP

The system includes FTP services. The FTP server is started via xinetd, see *xinetd(8)*. The following entry is the only active configuration entry in ***/etc/xinetd.conf*** :

Table 5-21 Sample ***/etc/xinetd.conf***** File**

File: */etc/xinetd.conf*

```
service ftp
{
      socket_type = stream
      protocol = tcp
      wait = no
      user = root
      server = /usr/sbin/vsftpd
      instances = UNLIMITED
}
```

An ftp server service is required for Z/Linux System Support and **vsftpd** is the recommended FTP client. The owner of the ftp directories and subdirectories will be set to root. The **vsftpd** uses several additional configuration files. In ***/etc/vsftpd.conf*** the configuration of the ftp daemon is specified. In addition, for access control, the classic ***/etc/ftpusers*** file is used. Users listed in the ***ftpusers*** file can NOT log in via FTP. This file initially contains all system ids and the root user. It can be augmented with other ids according to the local needs. The ***ftpusers*** file in not checked by the ftp daemon itself but by a PAM module. Please see the section "Required PAM configuration" (§3.12) for details. The setup of ***/etc/vsftpd.conf*** depends on the local needs. Please refer to *vsftpd.conf* (5) for details. The default configuration permits only anonymous FTP. This setting is therefore only suitable for distribution of public files for which no read access control is needed. Anonymous ftp servers are not allowed within EPA and will not be supported on SuSE Linux Enterprise Server 8. Disable anonymous FTP with the following setting in ***/etc/vsftpd.conf*** :

```
anonymous_enable=NO
```

An ***/etc/ftpusers*** file must exist, and it must list all users forbidden to use the ftp service. The forbidden accounts should include root, all system accounts, and any privileged accounts. Table 5-15 shows a sample ***/etc/ftpusers*** file.

The system administrator must modify the file ***/etc/vsftpd.conf***. The string to change is *ftpd_banner=Welcome…*, in the [greeter] section. The banner text should be typed in a single string.

Checklist Item: Anonymous FTP is disallowed.
Checklist Item: The file /etc/ftpusers exist and list all users forbidden to use the ftp service.
Checklist Item: The owner of the ftp directories and subdirectories set to root.
Checklist Item: The EPA approved warning banner will be in place for an FTP server.

Table 5-22 Sample *I/etc/ftpusers* File

File: */etc/ftpusers*
root
uucp
nobody
nobodyV
daemon
bin
uucp
uucpa
auth
cron
lp
tcb
adm
ris
wnn
esm
arsap
sys
sysadmin
netadm

5.5.5 File Sharing and Central Authentication

Network File System (NFS) is used to share file systems between UNIX and Linux systems, while Samba is used to share files between UNIX/Linux and Microsoft Windows-based systems. NFS has a history of security vulnerabilities. The use of NFS within EPA requires a waiver. If NFS is used, strong steps must be taken to ensure system and network security, as discussed in Section 5.5.5.1.

5.5.5.1 NFS

NFS will be disabled unless approval from the DCIOT has been received. SuSE Linux Enterprise Server 8 uses three different daemons for NFS clients and servers, all of which are normally started at boot time. **netfs** is used on client systems to mount remote NFS, SMB (Samba/Windows), and NPC (Netware) file systems. If no remote file systems need to be mounted, NFS can be disabled with the command:

```
sudo chkconfig netfs off
```

In addition, two daemons, **nfs** and **nfslock**, are used exclusively for NFS and can be disabled regardless of whether or not Samba or NPC are used; these daemons can be disabled as follows:

```
sudo chkconfig nfs off
sudo chkconfig nfslock off
```

The **autofs** daemon is used in conjunction with NFS to automount remote file systems. If NFS is not used, **autofs** too should be disabled:

```
sudo chkconfig autofs off
```

On systems where a waiver for NFS has been granted, steps must be taken to prevent unauthorized access to file systems as follows.

/etc/exports

Every entry in ***/etc/exports*** with read/write access must have an associated hostlist parameter. The hostlist parameter specifies what hosts are allowed to perform Network File System (NFS) mounts for read/write access on the exported file system. This also pertains to read only access. The *no_root_squash* parameter must not be used. This parameter allows the root user at the workstation performing the NFS mount of the file system to have root access to the file system. This creates a serious security vulnerability. Some form of a secure rpc authentication mechanism will be used to secure NFS.

rpc.nfsd and **rpc.mountd**

Z/Linux System Support will disable both **rpc.nfsd** and **rpc.mountd** on systems that are not using NFS. System security can further be tightened by disabling **amd**; however, doing so will also disable automatic mounting of local volumes. A determination on whether or not disabling **amd** is appropriate should be made by the system administrator and is dependent on the required functionality of the system.

/etc/hosts.allow and **portmap**

The system administrator can use the ***/etc/hosts.deny*** and ***/etc/hosts.allow*** file, described in Section 5.4.3, to restrict access to the portmapper program used by NFS to specific hosts, thereby preventing users on unauthorized systems from mapping the file systems to their servers. The ***/etc/hosts.deny*** file shown in Table 5-7 will already block all systems from all services, including **portmap**, unless those systems are explicitly listed in ***/etc/hosts.allow***. Table 5-16 shows an ***/etc/hosts.allow*** file modified to allow all EPA systems to access the portmapper, and therefore NFS. It is preferable to limit access to **portmap** to specific hosts.

Checklist Item: By default, NFS will be disabled.
Checklist Item: If NFS is used, NFS exports will **not** be writeable.
Checklist Item: If NFS is used, a secure rpc authentication mechanism will be in place.

Table 5-23 Sample */etc/hosts.allow* Configuration File with Portmap

File: */etc/hosts.allow*

```
#telnetd : 134.67.128.177
#ftpd :134.67.128.127
sshd: 134.67.
portmap: 134.67.128.177
#rlogind : 127.0.0.1
#
# If this machine is a server, uncomment one line below and change the
# name to match the X-terminal (or any X terminal that boots
# using tftp) DO NOT GENERALIZE THIS CONDITION!!!!! Add as many
# specific hosts as are required to boot the X terminals/diskless
# workstations.
#
# tftpd : diskless.workstation.region.epa.gov
```

5.5.5.2 NIS

Network Information Service (NIS) is not approved for installation or use on any system.

Checklist Item: By default, NIS will be disabled.

5.5.5.3 Samba

If file or print sharing between a SuSE Linux Enterprise Server 8 and Microsoft Windows systems is required, Samba can be used. Use of Samba within EPA requires a written business justification.

For detailed information on configuring and running Samba, see the URL http://us1.samba.org/samba/docs.

5.5.5.4 LDAP

OpenLDAP is an Open Source, free, cross-platform, client-server directory service provided with SuSE Linux Enterprise Server 8. If OpenLDAP is to be used within EPA, access must be restricted to trusted users and groups. LDAP should be implemented over Secure Sockets Layers (SSL).

Details on how to configure an LDAP server and clients under Linux can be found at the following
sites: http://en.tldp.org/HOWTO/LDAP-HOWTO/
http://en.tldp.org/HOWTO/LDAP-Implementation-HOWTO/index.html

Checklist Item: By default, LDAP will be disabled.

5.5.6 IP Configurations

SuSE Linux Enterprise Server 8 will not be used for routing within EPA. IP forwarding will be disabled on all SuSE Linux machines.

Checklist Item: By default, IP forwarding will be disabled.

The current kernel provided by SuSE Linux Enterprise Server 8 is configured with the *CONFIG_SYN_COOKIES* option set to allow, but not enable, SYN cookies in order to defeat a SYN flood attack. No action is needed by the system administrator in order to protect their systems. However, if the system administrator should ever need to build a custom kernel, this option should never be turned off.

5.5.7 Sendmail

SuSE Linux Enterprise Server 8 ships with Sendmail and is authorized for use in the EPA. Sendmail will be disabled unless explicitly required for normal operations. Sendmail can also be disabled from the command line by issuing the following command:

```
sudo chkconfig –level 2345 sendmail off
```

The system administrator should change the default **smtp** greeting by finding the following in ***/etc/sendmail.cf***:

```
O SmtpGreetingMessage=$j Sendmail $v/$Z; $b
```

and changing it to:

O SmtpGreetingMessage=$j Official Government Use Only; $b

The following line should be added to restrict mailq and expansion of aliases:
Opnoexpn,restrictmailq,restrictqrun,novrfy,authwarnings

5.5.8 SMTP

SMTP will be disabled unless explicitly required for normal operations. If an **SMTP** service is enabled, **SMTP** will be configured to ensure that all mail originates and terminates locally (prevent relaying).

Checklist Item: **SMTP** will be configured to prevent relaying.

5.5.9 Auditing / System Logging (syslogd)

Collecting data generated by system, network, application, and user activities is essential for analyzing the security of these assets and detecting signs of intrusion. Log files contain information about past activities. Because these files often provide the only indication of an intrusion, intruders often attempt to erase any evidence of their activities by removing or modifying the log files. For this reason, it is very important that log files be reviewed daily and kept adequately protected to make it as difficult as possible for intruders to change or remove them.

All system logs are stored by default in ***/var/log***. The file ***/var/log/secure*** is of particular importance, since it is where any and all security-related messages are likely to be recorded, including failed logins and all root activities (which include commands issued through the **sudo** facility). The default configurations of **inetd** (as described in Section 5.4.3), tcp wrappers (as described in Section 5.4.3.1), and OpenSSH (as described in Section 5.5.4.6) all log both successful connections and failed attempts in ***/var/log/secure***. This log must be checked daily for suspicious activity and should be reviewed immediately if the system administrator suspects something unusual is happening on the system. The default **syslog.conf** configuration should be acceptable for EPA use provided the guidelines for logging described in the aforementioned sections are followed.

System messages are logged in ***/var/log/messages***.

All system logs, both current and archived, in **/var/log** should have permissions set at *600* so that they can be read or written only by root.

Checklist Item: System logging will be enabled and **syslog.conf** complies with the Standard Configuration Document.

Checklist Item: Last failed login not displayed but the **login** program logs all failed login attempts in a system log file (via syslog).

Checklist Item: log files are readable only by root.
Checklist Item: All root access activities will be logged.
Checklist Item: All system errors will be logged.

5.5.10 System Services

Linux systems can be booted to different run levels as appropriate. The run levels used in SuSE Linux are:

0- Halt
1- Single User (maintenance)
2- Multi-user, NFS disabled
3- Multi-user
4- (unused)
5- Multi-user, boot to X11
6- Reboot

Under normal circumstances, EPA servers will boot into run levels 3 or 5.

Initialization scripts for the various services (daemons) run on the server are located in ***/etc/rc.d/rcx.d***, where *x* indicates the run level. For example, scripts to be executed when booting into run level 5 are located in ***/etc/rc.d/rc5.d.*** Scripts starting with the letter S are started at system initialization and are enabled, while ones starting with the letter K are killed, or disabled. For example, on a typical EPA system, in ***/etc/rc.d/rc5.d***, one would find the init script **S09sshd**, which starts the OpenSSH server daemon; and the script **K14sshd**, which kills the OpenSSH server daemon.

All scripts should be owned by root, with permissions set to *750* to prohibit unauthorized tampering.

To determine which services are to be started (and which are disabled) in each run level, the system administrator can execute the command:

```
sudo chkconfig –list
```

Table 5-5 shows a sample **chkconfig – list** output. As a general rule, all services that are not needed on a given server should be disabled for the highest level of security, using the command:

```
sudo chkconfig <service name> off
```

It should be noted that the **chkconfig** command only affects run levels 3, 4, and 5 by default. If the administrator wishes to enable or disable a service in a smaller group of run levels, or wishes to include other run levels in the command, the *–levels* argument must be used. For example:

```
sudo chkconfig –level 2345 sendmail off
```

disables Sendmail in run levels 2, 3, 4, and 5.

Services that should be disabled on most EPA systems include: **apmd, atd, ipchains, iptables, isdn, pppoe, rcp, rexec, rlogon, rstatd, rusersd, rwalld, rwhod, uucp, ypbind, yppasswdd,** and **ypserv.**

Services that should always be enabled on EPA systems include: **anacron, network, random, crond,** and **sshd. portmap** should be enabled in run levels 3 and 5 on any system acting as either a client or a server that is doing any sort of file, print, or authentication sharing, including NFS or Samba. **xfs** is required on all systems with X11 installed.

Leaving unnecessary services running will result in unnecessary ports left open, which is a potential security vulnerability.

5.5.10.1 Allowed Open Ports

Z/Linux System Support will contact their local security officer for information on which open ports are allowed. Z/Linux System Support will open only approved ports that are absolutely required for operation.

5.5.11 Configuration Tools

5.5.11.1 Tripwire

Tripwire is a consistency checker for Unix systems, including Linux. It takes a 'snapshot' of the filestore which can be periodically compared against a previous snapshot to detect any changes. It can use a variety of different algorithms to calculate the checksum or fingerprint of each file. Among the algorithms supplied are MD4, MD5, IDEA, Snefru, HAVAL and SHA.

The initial baseline created by Tripwire should be stored offline, ideally on media that cannot be erased or rewritten (e.g., CD-R), for regular comparison with the online system.

Details on how to configure Tripwire can be found in the Tripwire documentation.

5.5.11.2 System Security Monitoring

All servers connected to the EPA network must be monitored for security compliance and vulnerabilities. OTOP/NTSD provides software, documentation and support for Enterprise Security

Manager (ESM) and BindView Corporation's NOSadmin. Both provide system managers, administrators, and security administrators a tool for verifying a server's compliance to security-related, as well as other, standards.

ESM software and documentation are available at:
http://cfint.rtpnc.epa.gov/ntsdweb/security/index.cfm

BindView software and documentation are on local VABS servers in VOL3:\NATAPPS\ BINDVIEW.

For technical assistance on either ESM or Bindview, the EPA Call Center should be contacted at 866-411-4EPA (4372), or NIS Technical Support 919-541-5267.

5.5.11.3 linuxconf

The **linuxconf** system configuration utility is no longer installed by default in SuSE Linux Enterprise Server 8 due to serious security concerns. **linuxconf** is not approved for EPA use and will not be installed on any EPA systems.

All other graphical system configuration tools provided with SuSE Linux Enterprise Server 8 are acceptable for EPA use.

Checklist Item: By default, **linuxconf** is disabled.

5.5.11.4 Firewalls, ipchains and iptables

All firewall related packages must be removed from the system. Any exceptions to this must first be approved by the DCIOT. This includes the ipchains, and iptables packages. During installation, "No Firewall" must be selected on the firewall section of the install.

5.5.12 UNIX Security Checklist

The Unix Security Checklist has been developed to provide EPA system administrators with a comprehensive tool that will assist in ensuring that all systems are properly configured for connection on the EPA WAN. This check is mandatory and must be followed to ensure system security and integrity. See
http://intranet.epa.gov/dss/DSS_Customer/Security/Unix/unix-checklist.pdf.

5.6 STANDARD TOOLS

This section defines some standard tools utilized in the z/Linux environment. These tools are provided with z/Linux for zSeries and OS/390 and can be installed with the operating system.

5.6.1 TOP System Usage Monitor

GCC - Free C compiler

PERL - Freely available scripting language

5.6.2 GCC "C" Compiler

GCC is a free C compiler and is a standard part of the z/Linux installation.

5.6.3 PERL

PERL is a freely available scripting language commonly used on z/Linux systems, and is a standard part of the Linux installation.

Appendix A
EPA SOFTWARE INSTALLATION NOTES

This Appendix provides warnings, hints, and other information specific to the installation or upgrade of a z/Linux server in the EPA environment.

The z/Linux Operating System as shipped from SuSE is not secure. These security vulnerabilities must be eliminated. Outages can be avoided by implementing appropriate patches and configuration changes. As a result, the configuration changes documented in the z/Linux Standard Configuration Document must be implemented.

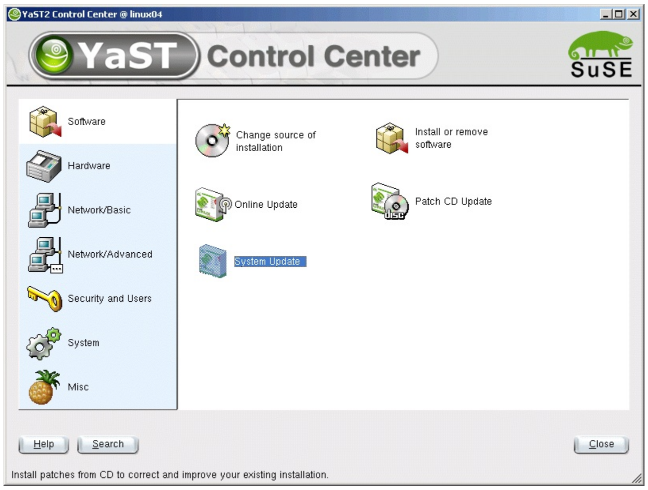
A.1 SOFTWARE UPGRADES

Numerous software upgrades for SuSE Linux Enterprise Server 8 have been released since the initial release of this version. It is essential to maintain system security and improve functionality and stability with these upgrades.

Current security vulnerabilities are also tracked by the CERT Coordination Center found at http://www.cert.org/.

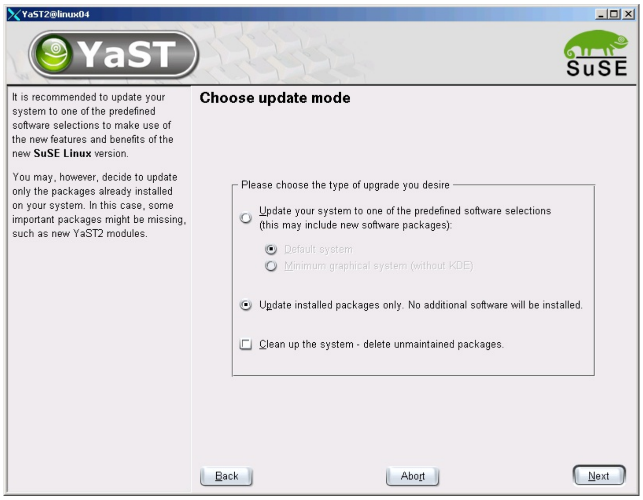
To do yast2-online-update, enter on an xwindow command line **YaST2**.

Select the **System Update** Icon:



Install patches from CD to correct and improve your existing installation.

On the **Back System Before Update** window, click **Next**
On the **Choose update mode** window, select **Update installed packages** only and click **Next**:



It is recommended to update your system to one of the predefined software selections to make use of the new features and benefits of the new **SuSE Linux** version.

You may, however, decide to update only the packages already installed on your system. In this case, some important packages might be missing, such as new YaST2 modules.

Choose update mode

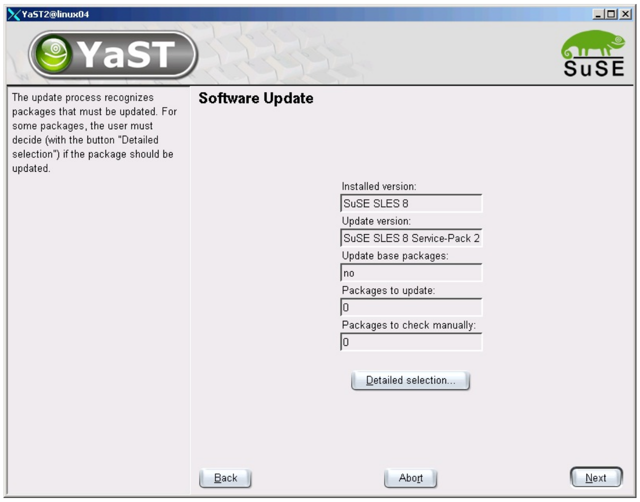
Please choose the type of upgrade you desire

○ Update your system to one of the predefined software selections (this may include new software packages):

- ● Default system
- ○ Minimum graphical system (without KDE)

● Update installed packages only. No additional software will be installed.

□ Clean up the system - delete unmaintained packages.



The update process recognizes packages that must be updated. For some packages, the user must decide (with the button "Detailed selection") if the package should be updated.

Software Update

Installed version: SuSE SLES 8
Update version: SuSE SLES 8 Service-Pack 2
Update base packages: no
Packages to update: 0
Packages to check manually: 0

Select the **Detailed selection...** button for a detailed list of available patches.

A.2 NEW SOFTWARE INSTALLS

To install a new version of SuSE Linux Enterprise Server 8:

1. Read the SuSE Installation Guide. A copy is available online at:
   – On z/Linux ***/usr/share/doc/packages/sles-inst-zseries_en/sles-inst-zseries_en.pdf***
   – On SuSE CD at **D:\docu\sles-inst-zseries_en.pdf**
2. Plan for the installation.
3. Perform a full backup of the server.
4. Perform the installation or upgrade.
5. Modify the system to match EPA OS Standard Configuration Document.
6. Apply all required security patches.
7. Perform a full backup after the completion of the upgrade or installation.

Important patch install note: Patches should be applied to the server after file configuration changes are made. At present, OS patches need to be applied at least monthly.

A.3 LIST OF FILES TO MODIFY

Table A-1, System Files Requiring Modification, contains a list of the files that need to be modified to become compliant with this UNIX OS Standard Configuration document.

Table A-1 System Files Requiring Modification

File	Reference Section
/etc/sysconfig/network/ifcfg-eth0	5.4.1
/etc/hosts	5.4.1
/etc/hosts.allow	5.4.3.3.1
/etc/hosts.deny	5.4.3.3.1
/etc/resolv.conf	5.4.3.4.1
/etc/xinetd.conf	5.4.3.1.1
/etc/issue	5.5.3
/etc/issue.net	5.5.3
/etc/motd	5.5.3
.rhosts	5.5.4.1.2
.netrc	5.5.4.1.2

File	Reference Section
/etc/hosts.equiv	5.5.4.1.1
/etc/pam.d/login	5.5.4.2
/etc/sudoers	5.5.4.6
/etc/snmpd.conf	5.5.4.7
/etc/cron.allow	5.5.4.8
/etc/ssh/sshd_config	5.5.3
/etc/X11/xdm/xaccess	5.5.4.10
/etc/opt/gnomes2/gdm.conf	5.5.4.10
/usr/share/config/kdmrc	5.5.4.10
/etc/ftpusers	5.5.4.3.10
/etc/exports	5.5.5.1
/etc/sendmail.cf	5.5.7
/etc/fstab	Appendix B.2, Appendix B.4

A.4 The Build Process

There are two phases to the z/Linux build process; the initial product build process and the product update/patch process.

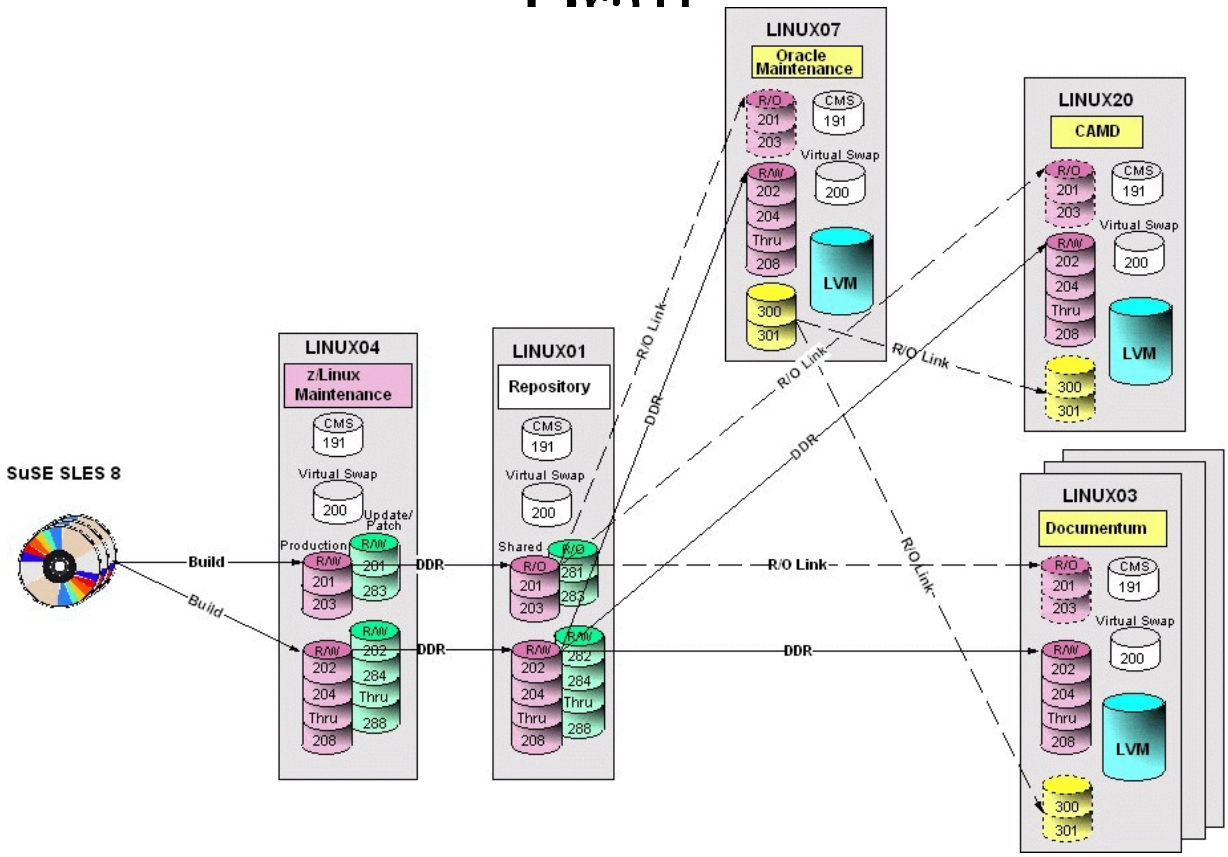
There are three types of z/Linux system, the test, repository, production z/Linux systems.

- The test z/Linux system is used for:
  - build and testing SuSE SLES8,
  - updating/patching and testing SuSE SLES 8.
- The repository z/Linux is used to hold the set of disks associated with the supported version/update/patch level of z/Linux system.
- The production z/Linux's are used by the various applications.

A.4.1 Product Build Process

The build process consists of the following steps:

1. The SuSE SLES 8 product is build and tested on the test Linux04 virtual machine. The system will reside on the set of R/W disks with addresses 20x.
2. The Linux04 virtual machine system disks are copied to a set of system disks on the repository Linux01 virtual machine. The R/W disks with addresses 201 and 203 are copied to R/O disks with addresses 201 and 203, respectively. The R/W disks with addresses 202 and 204 thru 208 are copied to R/W disks with addresses 202 and 204 thru 208, respectively.
3. When an application requests a z/Linux system, the Z/LINUX System Support group will create a virtual machine and z/Linux system from the repository Linux0x virtual machine. The repository Linux0x virtual machine system R/W disks are copied to a set of system R/W disks on the production z/Linux virtual machine. The R/W disks with addresses 202 and 204 thru 208 are copied to R/W disks with addresses 202 and 204 thru 208, respectively. The production is created with R/O link to the R/O disks with addresses 201 and 203.



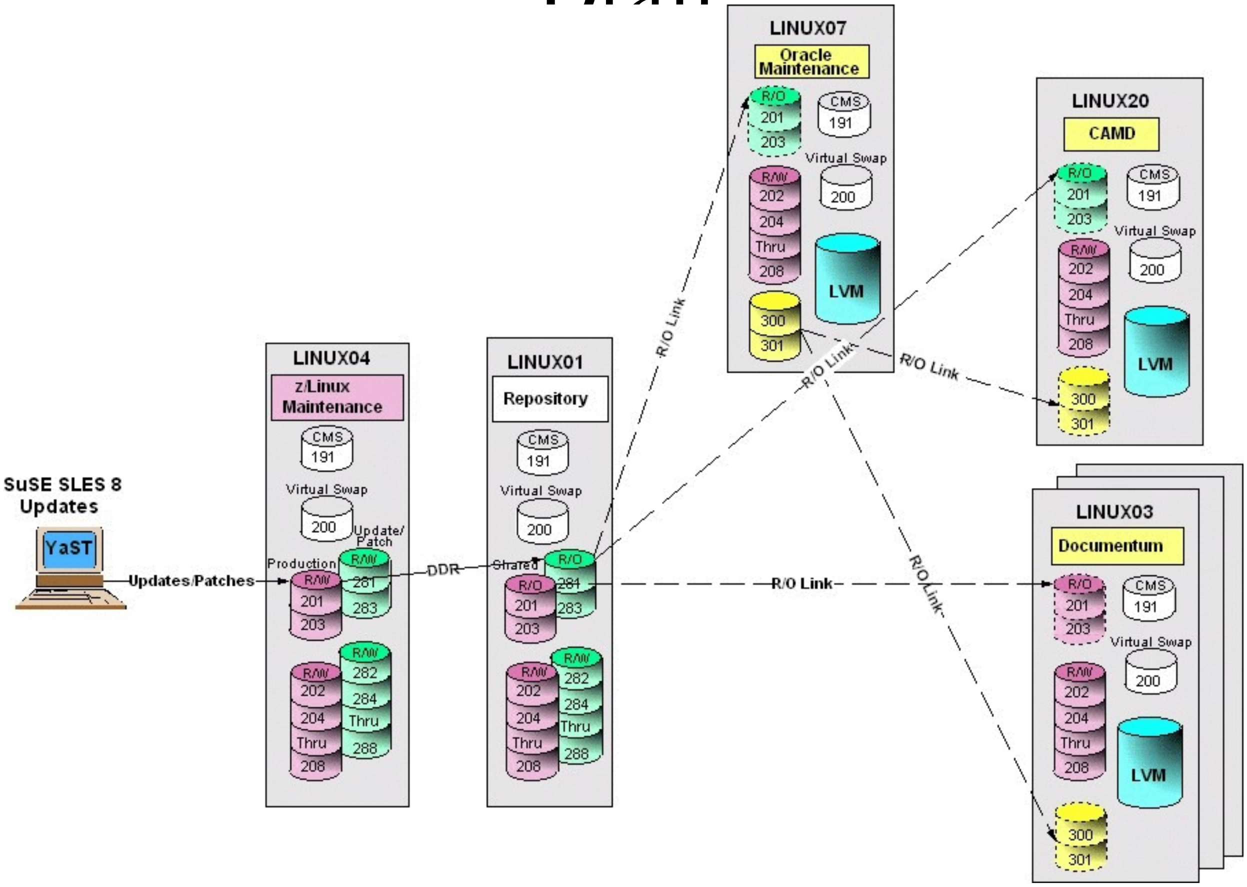
A.4.2 Product Update/Patch Process

The Update/Patch process consists of the following steps:

- The YaST Update tool on SuSE SLES 8 on the Linux04 virtual machine will be used to get and apply SuSE support. The system will reside on the set of R/W disks with addresses 20x.

- On the Linux04 virtual machine the updated production R/W disk is copied to a set R/O disks on the Linux01 virtual machineseparate from current production R/O disks. The R/W disks with addresses 201 and 203 are copied to R/O disks with addresses 281 and 283, respectively.

- The application will be notified via NCC Outage of the availability of the updated SuSE SLES 8 system. It will be up to the applications to contact the Z/LINUX System Support group to schedule the recycling of their z/Linux server. The Z/LINUX System Support group will then update the z/Linux R/O disk link and create a Change Control record for recycling the z/Linux server.



Draft

Appendix B
Secure Initial System Configuration

B.1 Minimum packages to be installed

The minimum package list is a starting place for a secure configuration. This list was gotten from a SuSE Linux System Enterprise Server 8 with the *certification-sles-eal2* package for a different platform. There is no implied level of security or certification, just a starting point.

Use **rpmqpack** to get a list of installed packages, and **rpm -e PACKAGE NAME ...** to remove all packages EXCEPT those listed here.

3ddiag
CheckHardware
SuSEfirewall2
UnitedLinux-build-key
aaa_base
aaa_skel
acl
alice-compat
argus
ash
at
attr
autoyast2
autoyast2-installation
bash
bc
bind9-utils
binutils
bzip2
cpio
cpp
cracklib
cron
cups-libs
curl
cyrus-sasl
db
devs
dhcpcd
dialog
diffutils
e2fsprogs
ed
eject
evlog
fbset
file
filesystem
fileutils
fillup
findutils
finger
fping
freetype
freetype2
gawk
gcal
gd
gdbm
glib
glibc
glibc-locale
gnuplot
gpg
gpm
grep
groff
gtk
gzip
hdparm
heimdal-lib
hotplug
howtoenh
hwinfo
ifnteuro
imlib
imwheel
intlfnts
[illegible]
iproute2
iptables
iputils
jfsutils
k_deflt
ksymoops
l2h-pngicons
less
libPropList
libgcc
libjpeg
liblcms
libmcrypt
libmng
libpcap
libpng
libstdc++
libtiff
libtool
libungif
libusb
libxcrypt
libxml
libxml2
libxslt
liby2util
listexec
logrotate
logsurfer
lsof
lukemftp
lvm
m4
mailx
man
man-pages
mdadm
mesa
mesaglu
mesaglut
mesasoft
mhash
mkisofs
mktemp
modutils
mon
mtr
mtr-gtk
nagios
nagios-nsca
nagios-plugins
ncurses
nessus
net-tools
netcat

netcfg
nmap
openldap2-client
openmotif
openssh
openssh-askpass
openssl
pam
pam-modules
parted
patch
pciutils
pcre
pdksh
perl
perl-Convert-BER
perl-Crypt-DES
perl-Digest-HMAC
perl-Digest-SHA1
perl-HTML-Parser
perl-HTML-Tagset
perl-Mon
perl-Net-SNMP
perl-SNMP
perl-Time-Period
perl-Tk
perl-URI
perl-XML-DOM
perl-XML-Generator
perl-gettext
perl-libwww-perl
permissions
plotutils
popt
portmap
postfix
postgresql-libs
powertweak
procmail
providers
ps
qt3
raidtools
readline
recode
reiserfs
rpm
rsh
s390-tools
saint
sash
scanlogd
scpm
scsi
seccheck
sed
sh-utils
shadow
sitar
sles-release
snort
src_vipa
star
suse-build-key
sysconfig
syslogd
sysstat
sysvinit
tar
tcl
tclx
tcsh
telnet
terminfo
texinfo
textutils
timezone
tix
tk
tripwire
ttmkfdir
ucdsnmp
unclutter
unixODBC
utempter
util-linux
varmon
vim
vsftpd
w3m
w3m-inline-image
webalizer
wget
x3270
xaw3d
xbanner
xdmbgrd
xf86
xf86_glx
xf86tools
xfntscl
xlock
xosview
xscsi
xshared
xtermset
yast2
yast2-backup
yast2-bootloader
yast2-control-center
yast2-core
yast2-country
yast2-firewall
yast2-inetd
yast2-installation
yast2-ldap-client
yast2-mail
yast2-mouse
yast2-ncurses
yast2-network
yast2-nfs-client
yast2-nfs-server
yast2-nis-client
yast2-nis-server
yast2-online-update
yast2-packagemanager
yast2-packager
yast2-pam
yast2-powertweak
yast2-printer
yast2-printerdb
yast2-profile-manager
yast2-qt
yast2-restore
yast2-runlevel
yast2-security
yast2-storage
yast2-sysconfig
yast2-theme-SuSELinux
yast2-trans-en_US
yast2-transfer
yast2-tune
yast2-update
yast2-users
yast2-x11
yast2-xml
zlib

B.2 Disable service

Note: The system runlevel as specified in the ’initdefault’ entry in /etc/inittab MUST remain at the default setting of ’3’ for these steps to be valid.

Only the following servers are allowed for runlevel 3:

- random
- network
- syslog
- sshd
- postfix
- atd
- cron
- kbd
- lpd
- rpmconfigcheck
- hwscan
- xinetd

All others MUST be removed with **insserv -r ServiceName**.

B.3 Remove setuid/setgid root settings from binaries

Use of the setuid bit on binaries (to run with root privileges) MUST be limited to those shown in the following list. The other binaries that were installed ”setuid root” MUST have this bit removed. ’root’ can still run these binaries normally, but they are not available for ordinary users.

- /bin/ping
- /bin/su
- /usr/bin/at
- /usr/bin/chage
- /usr/bin/chfn
- /usr/bin/chsh
- /usr/bin/crontab
- /usr/bin/lpq
- /usr/bin/lpr
- /usr/bin/lprm
- /usr/bin/lpstat
- /usr/bin/passwd

There is also a number of SGID files on the system that are needed:

- /usr/sbin/postdrop
- /usr/sbin/postqueue

For informational purposes, here is a non authoritative list of programs that have their setuid or setgid bit removed:

- /bin/ping6
- /bin/umount
- /sbin/unix2_chkpwd
- /sbin/unix_chkpwd
- /usr/bin/expiry
- /usr/bin/mandb
- /usr/bin/newgrp
- /usr/bin/ssh
- /usr/bin/wall
- /usr/bin/write
- /usr/lib/pt_chown
- /usr/sbin/lpc
- /usr/sbin/utempter

Similarly, the setgid bit MUST NOT be used to give group ”root” privileges to any binary. The SuSE permission mechanism MUST be used to set permission bits appropriately. First make sure that no SUID/SGID programs are present on the system:

```
find / \( ! -fstype ext3 -prune -false \) -o \
-type f \( -perm -4000 -o -perm -2000 \) \
-exec chmod u-s,g-s {} \; -print
```

Then run **chkstat -set /etc/permissions.d** to set the needed SUID and SGID bits.
Make sure that ***/etc/sysconfig/security*** has the following two variables set:

- CHECK_PERMISSIONS=set
- PERMISSION_SECURITY="easy local"

Appendix C
Monitoring, Logging & Audit

C.1 Reviewing the system configuration

It is recommended that you review the system's configuration at regular intervals to verify if it still agrees with the secure configuration. This primarily concerns those processes that may run with 'root' privileges. The permissions of the device files /dev/* MUST NOT be modified. In particular, review settings in the following files and directories to ensure that the contents and permissions have not been modified:

/etc/at.allow
/etc/at.deny
/etc/cron.d/*
/etc/cron.daily/*
/etc/cron.hourly/*
/etc/cron.monthly/*
/etc/cron.weekly/*
/etc/crontab
/etc/ftpusers
/etc/group
/etc/gshadow
/etc/hosts
/etc/init.d/*
/etc/inittab
/etc/ld.so.conf
/etc/login.defs
/etc/modules.conf
/etc/pam.d/*
/etc/passwd
/etc/securetty
/etc/security/pam_pwcheck.conf
/etc/security/pam_unix2.conf
/etc/shadow
/etc/ssh/ssh_config
/etc/ssh/sshd_config
/etc/sysconfig/*
/etc/vsftpd.conf
/etc/xinetd.conf
/usr/lib/cracklib_dict.*
/var/spool/atjobs/*
/var/spool/cron/*
/var/spool/cron/allow
/var/spool/cron/deny

Use the commands faillog and lastlog to detect unusual patterns of login attempts or an unexpectedly large number of login failures. Also verify the output of the following commands (run as 'root'):

```
atq
crontab -l
find / \( -perm -4000 -o -perm -2000 \) -ls
find / \( -type f -o -type d -o -type b \) -perm -0002 -ls
find /bin /boot /etc /lib /sbin /usr \
! -type l \( ! -uid 0 -o -perm +022 \)
```

C.2 System logging and accounting

System log messages are stored in the ***/var/log/*** directory tree in plain text format, most are logged through the *syslogd(8)* and *klogd(8)* programs, which MAY be configured via the file ***/etc/syslog.conf***.

The *logrotate(8)* utility, launched from ***/etc/cron.daily/logrotate***, starts a fresh log file every week or when they reach a maximum size and automatically removes or archives old log files. You MAY change the configuration files ***/etc/logrotate.conf*** and ***/etc/logrotate.d/**** as required. In addition to the syslog messages, various other log files and status files are generated in ***/var/log*** by other programs:

File	Source
YaST2	Directory for YaST2 log files
boot.msg	Messages from system startup
faillog	Failed log ins of known users, (see *faillog(8)*)
lastlog	Last successful log in (see *lastlog(8)*)
vsftpd.log	Transaction log of the VSFTP daemon
localmessages	Written by syslog
mail	Written by syslog, contains messages from the MTA (postfix)
messages	Written by syslog, contains messages from **su** and **ssh**
news/	syslog news entries (not currently supported)
warn	Written by syslog
wtmp	Written by the PAM susbystem, see *who(1)*
xinetd.log	Written by **xinetd**, logging all connections

Please see *syslog(3)*, *syslog.conf (5)* and *syslogd(8)* man pages for details on syslog configuration.

The *ps(1)* command can be used to monitor the currently running processes. Using ps faux will show all currently running processes and threads.

C.3 System configuration variables in /etc/sysconfig

The system uses various files in ***/etc/sysconfig*** to configure the system. Most files in this directory tree contain variable definitions in the form of shell variables that are either read by the **rc** scripts at system boot time or are evaluated by the **SuSEconfig** command and used as input to re-write other configuration files on the system.

The following is a brief overview of the security relevant files, including the specification of permitted changes.

In the secure configuration, no changes are permitted that would require running the **SuSEconfig** command to rewrite other configuration files. You MAY run **SuSEconfi**g, but it will have no effect on the secure configuration.

suseconfig

This file specifies global configuration variables. Most notably ENABLE SUSECONFIG, which specifies whether **SuSEconfig** is allowed to modify other configuration files based on the variables in ***/etc/sysconfig***.

Security relevant entries that MUST NOT be changed are:

ENABLE_SUSECONFIG="yes" Is SuSEconfig allowed to modify configuration files?
MAIL_REPORTS_TO="root" Where are system status mails sent to
CWD_IN_ROOT_PATH="no" There MUST NOT be an entry for the current directory
CWD_IN_USER_PATH="no" There MUST NOT be an entry for the current directory

security

Specifies the operation mode and the configuration file for the SuSE permission system. Read by the *chkstat(8)* program which is run automatically by yast2 after installation of new software. The following settings MUST NOT be changed:

CHECK_PERMISSIONS=set
PERMISSION_SECURITY="easy local"

cron

Configures standard system **cron** jobs, like deletion of old files in ***/tmp*** or update of the man databases. The settings are read by the shell scripts ***/etc/cron.daily/****. Security relevant variables are the following settings which MUST NOT be changed:

MAX_DAYS_IN_TMP=0 How many days can files stay in /tmp
TMP_DIRS_TO_CLEAR="***/tmp /var/tmp***" Which temporary directories are checked
OWNER_TO_KEEP_IN_TMP="root" Ids for which files will not be erased
CLEAR_TMP_DIRS_AT_BOOTUP="no" No cleaning of temp directories at boot

language

Sets up the default locale. This MUST NOT be changed, non-root users MAY override these default settings in their shell profiles.

backup

Configures the backup of the RPM database. MAY be changed.

boot

Configures the verbosity and interaction level of the boot process for debugging. Read by bootup scripts in ***/etc/init.d/***. MAY be changed.

displaymanager

This would configure the display manager for a workstation. Not currently supported.

kernel

Configures modules to be installed in the **initrd** for system boot. MUST NOT be changed.

clock

Configures time zone and system clock, read during system boot. MAY be changed.

proxy

Configures global variables for the use of proxies. Not currently supported.

windowmanager

Would select the window manager on a workstation. Not currently supported.

sysctl

Configures some system variables for the boot process. The following are security relevant and MUST NOT be changed:

IP_DYNIP=no The system only has a static address
IP_TCP_SYNCOOKIES=yes Syn Flood protection
IP_FORWARD=no Has to be set to yes if the system acts as a router.
ENABLE_SYSRQ=no System request key MUST be disabled.

java

Would configure the JavaTMrun time environment if installed. Not currently supported.

mail

Configures the MTA. Security relevant variables that MUST NOT be changed are:

SMTPD_LISTEN_REMOTE="no" If set to yes, **SuSEconfig** will tell postfix to accept remote connections.

printer

Sets the default printer. MUST NOT be changed, but non-root users may override the setting in their shell profiles.

news

Usenet news / NNTP settings. Not currently supported.

console

Sets up the console configuration (font, code page, frame buffer). MUST NOT be changed.

keyboard

Sets up the console keyboard (repeat rate, layout, number of virtual consoles). MAY be changed.

mouse

Sets up the mouse type. Not currently supported.

lvm

Sets up LVM. Not currently supported.

network

This directory contains the networking configuration and scripts for the interfaces and routes. MAY be modified as needed, but IP addresses MUST be static (no DHCP).

syslog

Configures the syslog daemon. MAY be changed.

SuSEfirewall2

Configures the SuSE firewall. Not currently supported.

hotplug

Configures dynamically attached devices (USB, Firewire). Not currently supported.

ssh

Configures command line options for the SSH daemon. MUST NOT be changed.

postfix

Configures the basic MTA setup. MUST NOT be changed.

bootloader

Configures the type of bootloader to use and where to store the boot record. MUST NOT be changed.

Appendix D
Pluggable Authentication Module (PAM) configuration

D.1 Introduction to PAM configuration

The PAM subsystem is responsible for maintaining passwords and other authentication data. Because this is a security critical system, understanding how it works is very important. In addition to the *pam*(8) manual page, full documentation is available in ***/usr/share/doc/packages/pam/text/***, and includes *"The Linux-PAM System Administrator's Guide"* (*pam.txt*) as well as information for writing PAM applications and modules. Detailed information about modules is available in ***/usr/share/doc/packages/pam/modules/README.pam***, as well as manual pages for individual modules, i.e. *pam_pwcheck*(8).

The PAM configuration is stored in the ***/etc/pam.d/*** directory. Note that the documentation refers to a file ***/etc/pam.conf*** which is not used by SLES (PAM was compiled to ignore this file if the ***/etc/pam.d/*** directory exists).

Each service (application) that uses PAM for authentication uses a *service-name* to determine its configuration, stored in the file ***/etc/pam.d/****service-name*. The special *service-name* **other** (case insensitive) is used for default settings if there are no specific settings.

The configuration file for the service contains one entry for each module, in the format:

```
module-type control-flag module-path args
```

Comments MAY be used, extending from '#' to the end of the line, and entries MAY be split over multiple lines, using a backslash at the end of a line as a continuation character.

The *module-type* defines the type of action being done. This can be one of four types:

auth

Authenticates users (determines that they are who they claim to be). It can also assign credentials, i.e. additional group memberships beyond those specified through ***/etc/passwd*** and ***/etc/groups*** - this additional functionality MUST NOT be used.

account

Account management not related to authentication, i.e. restricting access based on time of day, available system resources or the location of the user (network address or system console).

session

Manages resources associated with a service by running specified code at the start and end of the session. Typical usage includes logging and accounting, and initialization such as auto mounting a home directory.

password

Used for updating the password (or other authentication token), i.e. when using the *passwd*(1) utility to change it.

The *control-flag* specifies the action that will be taken based on the success or failure of an individual module. The modules are stacked (executed in sequence), and the *control-flags* determine which final result (success or failure) will be returned, thereby specifying the relative importance of the modules.

Stacked modules are executed in the order specified in the configuration file. The *control-flag* can be specified as either a single keyword, or alternatively with a more elaborate syntax that allows greater control. SLES uses only the single keyword syntax by default.

required

If this module returns a failure code, the entire stack will return failure. The failure will be reported to the application or user only after all other modules in the stack have been run, to prevent leakage of information (for example, ask for a password even if the entered username is not valid).

requisite

Same as **required**, but return failure immediately, not executing the other modules in the stack. Can be used to prevent a user from entering a password over an insecure connection.

sufficient

Return success immediately if no previous **required** modules in the stack have returned failure. Do not execute succeeding modules.

optional

The return code of this module is ignored, except if all other modules in the stack return an indeterminate result (PAM IGNORE).

The *module-path* specifies the filename of the module to be run (relative to the directory ***/lib/security/***, and the optional *args* are passed to the module - refer to the module’s documentation for supported options.

Appendix E
ONLINE FILES REFERENCE

The following are a list of online files referenced in the z/Linux Standard Configuration Document; they are as follows (but not limited to):

support_dss@epamail.epa.gov

http://intranet.epa.gov/dss/DSS_Customer/SCD/page1.html

Appendix F
SYSTEM ADMINISTRATOR SKILLS REQUIREMENTS

One of the following qualifications must be met for someone to qualify as an SuSE Linux Enterprise Server system administrator:

- Completion of two weeks of formal system administration training for the SuSE Linux operating system. This course must also cover TCP/IP configuration for the specific platform. The following SuSE Training (http://www.suse.com/us/business/services/training/susetrain) course covers the recommendations:

  – **SuSE Linux Enterprise Server 8**

- Over one year of full-time experience in Linux system administration in a TCP/IP network environment.

- Over three years of full-time experience in one of the following fields: computer system administration (e.g., UNIX, VMS, Novell, Pathworks, IBM Mainframe) and applications or systems programming. An undergraduate degree or equivalent formal training in the computer or information sciences.

Appendix G
KEY CONTACTS AND UPDATES TO DOCUMENT

The z/Linux Standard Configuration document is a living document. As such, updates to the key contacts listing and the document in general will be made as necessary.

Table H-1 contains a list of key contacts.

Table H-1 Key Contacts

Function	Contact Name	Phone
z/Linux System Support Center, RTP	Technical Support Specialist	919-767-7256

NOTE: The key contact table above is current as of the date of this document, but is subject to change.

Appendix H
ACRONYM LIST

-A-

ADVFS	Advanced File System
ARP	Address Resolution Protocol
ASET	Author System for Education and Training
ASO	Advanced Security Option
ATM	Asynchronous Transfer Mode

-B-

BSD	Berkeley Software Distribution
BSM	Basic Security Module

-C-

CD	Compact Disc
CDE	Common Desktop Environment
CDFS	Compact Disc File System
CD-ROM	Compact Disc - Read Only Memory
CERT	Computer Emergency Response Team
CP	Central Processor
CPU	Central Processing Unit
CRC	Computer Resource Control, Inc.
CTC	Channel to Channel

-D-

DASD	Direct Access Storage Device
DCIOT	Deputy Chief Information Officer for Technology
DHCP	Dynamic Host Configuration Protocol
DLS	Document Library Services
DNS	Domain Name Service/System
DSS	Decision Support System; Data Set Services

-E-

ECKD	Extended Count-Key-Data
EOF	End of File; Evaluated Optional Feature
EPA	Environmental Protection Agency
ESA	Enterprise System Architecture
ESM	Enterprise Security Manager
ESRI	Environmental Systems Research Institute

-F-

FTP	File Transfer Protocol; Forms Translator Program

-G-

GCC	GNU Compiler Collection
GID	Group ID
GNU	GNU's Not Unix
GUI	Graphical User Interface

-H-

HAVAL	One-Way Hashing Algorithm with Variable Length of Output
HDSD	Headquarters and Desktop Services Division

-I-

IDEA	International Data Encryption Algorithm
IFL	Integrated facility for Linux
IP	Information Providers; Internet Protocol
IPL	Initial Program Loader
ISO	Information Security Officer
IUCV	Inter-User Communications Vehicle

-K-

KDE	Contemporary desktop environment for Linux

-L-

LAN	Local Area Network

LCS	LAN Channel Station
LDAP	Lightweight Directory Access Protocol
LPAR	Logical Partition
LVM	Logical Volume Manager

-M-

MB	Megabyte
MD4	Message Digest hash algorithm 4
MD5	Message Digest hash algorithm 5
MTA	Message Transfer Agents

-N-

NASA	National Aeronautics and Space Administration
NCA	Network Cache & Accelerator
NCC	National Computer Center
NCF	Network Control Facility
NFS	Network File System
NIS	Network Infrastructure Services
NNTP	Network News Transfer Protocol
NPC	NetWare Core Protocol
NSF	Network Supervisory Function; National Science Foundation
NTSD	National Technology Services Division

-O-

ONC	Open Network Computing
OS	Operating System
OSA	Open System Adapter
OTOP	Office Of Technology Operations & Planning

-P-

PAM	Pluggable Authentication Modules
PERL	Practical Extraction and Report Language

-Q-

QDIO	Queued Direct I/O

-R-

RAM	Random Access Memory
RFC	Requests for Comments
RPC	Remote Procedure Call
RPM	Redhat Package Manager for Linux
RSH	Remote Shell

-S-

SA	System Analyst; System Administrator
SAIC	Scientific Applications International Corporation
SCD	Standard Configuration Document
SCSI	Small Computer System Interface
SEWPII	Scientific & Engineering Workstation Procurement 2
SGID	Set Grout ID in Linux
SHA	Secure Hash Algorithm
SIRMO	Senior Information Resources Management Official
SMB	Server Message Block in Windows
SMTP	Simple Mail Transport Protocol
SLES	SuSE Linux System Enterprise Server
SNMP	Simple Network Management Protocol
SRM	Systems Resource Manager
SSH	Secure Shell
SSL	Secure Socket Layer
SYSTAT	Informational service in Linux
SYN	Synchronous idle message
SUID	Set User ID in Linux

-T-

TCP	Terminal/Controller Processor
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TOP	Free system resource monitor in Linux
TSR	Telecommunications Service Request
TSSMS	Time Sharing Services Management System

-U-

UID	User ID
UMASK	User file-creation mask
URL	Universal Resource Locator
USB	Universal Serial Bus (Intel)
USR	User Service Request

-V-

VABS	Value-Added Backbone Services
VM	Virtual Machine
VSFTP	Very Secure FTP

-W-

WAN	Wide Area Network
WCF	Working Capital Fund
WIC	Washington Information Center

-X-

XDCMP	XDMCP protocol allows remote displays to be managed by GDM